The Automorphism Group of a Finite p-Group is Almost Always a p-Group

Geir T. Helleloid
Department of Mathematics, Bldg. 380
Stanford University
Stanford, CA 94305-2125
geir@math.stanford.edu

Ursula Martin
Department of Computer Science
Queen Mary University of London
Mile End Road
London E1 4NS, UK
Ursula.Martin@dcs.qmul.ac.uk

February 2, 2008

Abstract

Many common finite p-groups admit automorphisms of order coprime to p, and when p is odd, it is reasonably difficult to find finite p-groups whose automorphism group is a p-group. Yet the goal of this paper is to prove that the automorphism group of a finite p-group is almost always a p-group. The asymptotics in our theorem involve fixing any two of the following parameters and letting the third go to infinity: the lower p-length, the number of generators, and p. The proof of this theorem depends on a variety of topics: counting subgroups of a p-group; analyzing the lower p-series of a free group via its connection with the free Lie algebra; counting submodules of a module via Hall polynomials; and using numerical estimates on Gaussian coefficients.

1 Introduction

The goal of this paper is to prove that, in a certain asymptotic sense, the automorphism group of a finite p-group is almost always a p-group. A weaker version of this result was announced by the second author in [21], but this paper contains the first published proof.

The result may not seem entirely plausible at first, as many common finite p-groups have an automorphism group that is not a p-group. Examples in-

Order	$p = 2$	$p = 3$	$p = 5$
p^3	3 of 5	0 of 5	0 of 5
p^4	9 of 14	0 of 15	0 of 15
p^5	36 of 51	0 of 67	1 of 77
p^6	211 of 267	30 of 504	65 of 685
p^7	2067 of 2328	2119 of 9310	11895 of 34297

Table 1: The proportion of p-groups of a given order whose automorphism group is a p-group.

clude: abelian p-groups, unless $p = 2$ and the type of the group has repeated parts (see Macdonald [19, Chapter II, Theorem 1.6]); the Sylow-p subgroup of $\mathrm{GL}(n, \mathbb{F}_p)$ for p odd (see Gibbs [8]); and the extraspecial p-groups (see Winter [33]). Furthermore, Bryant and Kovács [3] show that any finite group occurs as the quotient $A(H)$ of the automorphism group of some finite p-group H, where $A(H)$ is as defined below. Our result seems to say that most p-groups are complicated and unnatural-looking and that familiar examples are far from typical.

It is reasonably easy to find finite 2-groups whose automorphism group is a 2-group: $\mathbb{Z}_{2^n}$, the dihedral 2-group D_{2^n} ($n \geq 3$), and the generalized quaternion group Q_{2^n} ($n \geq 4$) are common examples, while Newman and O'Brien [24] offer three more infinite families. It is more difficult to find finite p-groups whose automorphism groups are p-groups when p is odd. In [14], Horoševskiĭ constructs such a p-group with nilpotence class n for each $n \geq 2$ and such a p-group on d generators for each $d \geq 3$. Furthermore, Horoševskiĭ shows in [14] and [15] that for any prime p, if $H_1, H_2, \ldots, H_n$ are finite p-groups whose automorphism groups are p-groups, then the automorphism group of the iterated wreath product $H_1 \wr H_2 \wr \cdots \wr H_n$ is also a p-group. Otherwise, most known examples arise from complicated and unnatural-looking constructions (see Webb [30]). A survey on the automorphism groups of finite p-groups, including a comprehensive list of examples in the literature of finite p-groups whose automorphism groups are p-groups, can be found in [11].

In a computational vein, Eick, Leedham-Green, and O'Brien [4] describe an algorithm for constructing the automorphism group of a finite p-group. This algorithm has been implemented by Eick and O'Brien in the GAP package AutPGroup [6]. Compiled with the gracious help of Eamonn O'Brien (personal communication) and the GAP packages AutPGroup and SmallGroups [6], Table 1 summarizes data on the proportion of small p-groups whose automorphism group is a p-group. (More information about the SmallGroups package can be found in Besche, Eich and O'Brien [1].)

Of course, the meaning of the statement "The automorphism group of a finite p-group is almost always a p-group" depends on the asymptotic interpretation of "almost always." Probably the most natural interpretation is to consider all p-groups of order at most p^n and let n go to infinity. However, this is not the sense

of our result, and indeed, the question remains open for this interpretation (see Mann [20, Question 9]). The precise statement of our main theorem depends on the *lower p-series* of a group. The lower p-series will be defined in Section 2; for the moment, it suffices to say that the lower p-series is a central series with elementary abelian factors and that the *lower p-length* of a group is the number of non-identity terms in the associated lower p-series. The main theorem of this paper may be concisely stated as follows.

Theorem 1.1. *Fix a prime p and positive integers d and n. Let $r_{d,n}$ be the proportion of p-groups minimally generated by d elements and with lower p-length at most n whose automorphism group is a p-group. If $n \geq 2$, then*

$$\lim_{d\to\infty} r_{d,n} = 1.$$

If $d \geq 5$, then

$$\lim_{n\to\infty} r_{d,n} = 1.$$

If $n = 2$ and $d \geq 10$, or $n \geq 3$ and $d \geq 6$, or $n \geq 10$ and $d \geq 5$, then

$$\lim_{p\to\infty} r_{d,n} = 1.$$

The proof of Theorem 1.1 breaks down into three parts, which are presented in Sections 2, 5, and 6, and are assembled to prove Theorem 1.1 in Section 7. In the remainder of this section, we will outline the structure of the proof.

The first step is to connect the enumeration of finite p-groups to an analysis of certain subgroups and quotients of free groups. Let F be the free group on d generators and let F_n be the n-th term in the lower p-series of F. It turns out that the action of $\mathrm{Aut}(F/F_{n+1})$ on F_n/F_{n+1} induces an action of $\mathrm{GL}(d,\mathbb{F}_p)$ on F_n/F_{n+1}, and the $\mathrm{Aut}(F/F_{n+1})$-orbits on the normal subgroups of F_n/F_{n+1} are also the $\mathrm{GL}(d,\mathbb{F}_p)$-orbits.

For any finite p-group H, write $A(H)$ for the group of automorphisms of $H/\Phi(H)$ induced by $\mathrm{Aut}(H)$, where $\Phi(H)$ is the Frattini subgroup of H. We shall see that if $A(H)$ is a p-group then so is $\mathrm{Aut}(H)$; in fact, our main goal is to prove, in some sense, that $A(H)$ is usually trivial. In Section 2, after defining and investigating the lower p-series, we prove the following theorem.

Theorem 1.2. *Fix a prime p and integers $d, n \geq 2$. Let F be the free group on d generators and define the following sets:*

$$\begin{aligned}
\mathcal{A}_{d,n} &= \{\textit{normal subgroups of } F/F_{n+1} \textit{ lying in } F_2/F_{n+1}\}\\
\mathcal{B}_{d,n} &= \{\textit{normal subgroups of } F/F_{n+1} \textit{ lying in } F_2/F_{n+1}\\
&\qquad \textit{and not containing } F_n/F_{n+1}\}\\
\mathcal{C}_{d,n} &= \{\textit{normal subgroups of } F/F_{n+1} \textit{ lying in } F_n/F_{n+1}\}\\
\mathcal{D}_{d,n} &= \{\textit{normal subgroups of } F/F_{n+1} \textit{ contained in the}\\
&\qquad \textit{regular } \mathrm{GL}(d,\mathbb{F}_p)\textit{-orbits in } \mathfrak{C}_{d,n}\}
\end{aligned}$$

$$\begin{aligned}
\mathfrak{A}_{d,n} &= \{\mathrm{Aut}(F/F_{n+1})\text{-}orbits\ in\ \mathcal{A}_{d,n}\} \\
\mathfrak{B}_{d,n} &= \{\mathrm{Aut}(F/F_{n+1})\text{-}orbits\ in\ \mathcal{B}_{d,n}\} \\
\mathfrak{C}_{d,n} &= \{\mathrm{Aut}(F/F_{n+1})\text{-}orbits\ in\ \mathcal{C}_{d,n}\} = \{\mathrm{GL}(d,\mathbb{F}_p)\text{-}orbits\ in\ \mathcal{C}_{d,n}\} \\
\mathfrak{D}_{d,n} &= \{regular\ \mathrm{GL}(d,\mathbb{F}_p)\text{-}orbits\ in\ \mathcal{C}_{d,n}\}.
\end{aligned}$$

Then there is a well-defined map $\pi_{d,n} : \mathfrak{A}_{d,n} \to \{$*finite p-groups*$\}$ *given by* $L/F_{n+1} \mapsto F/L$, *where* $L/F_{n+1} \in \mathcal{A}_{d,n}$. *Furthermore* $\pi_{d,n}$ *induces bijections*

$$\begin{aligned}
\mathfrak{A}_{d,n} &\leftrightarrow \{p\text{-}groups\ of\ lower\ p\text{-}length\ at\ most\ n \\
&\qquad\qquad and\ minimally\ generated\ by\ d\ elements\} \\
\mathfrak{B}_{d,n} &\leftrightarrow \{p\text{-}groups\ of\ lower\ p\text{-}length\ n \\
&\qquad\qquad and\ minimally\ generated\ by\ d\ elements\} \\
\mathfrak{D}_{d,n} &\leftrightarrow \{subgroups\ H\ in\ \pi_{d,n}(\mathfrak{C}_{d,n})\ with\ A(H) = 1\}.
\end{aligned}$$

Recall that a regular orbit is one in which every point has trivial stabilizer. Note that as a result of Theorem 1.2, it will be enough to show that $|\mathfrak{A}_{d,n}|/|\mathfrak{D}_{d,n}|$ goes to 1 under the relevant limits.

Section 3 follows with an examination of the structure of F_n/F_{n+1} that will be needed in Section 5. Section 4 contains combinatorial estimates, including bounds on Gaussian coefficients, that will be needed in Sections 5 and 6. Finally, the second and third steps of the proof of Theorem 1.1 are summarized in Theorems 1.3 and 1.4 and are proved in Sections 5 and 6. The terms $C(p)$ and $D(p)$ that appear in Theorems 1.3 and 1.4 are functions of p which tend to 1 as $p \to \infty$.

Theorem 1.3. *Fix a prime* p *and integers* d *and* n *so that either* $n \geq 3$ *and* $d \geq 6$ *or* $n \geq 10$ *and* $d \geq 5$. *Let* F *be the free group on* d *generators and let* d_n *be the rank of* F_n/F_{n+1}. *Then*

$$1 \leq \frac{|\mathfrak{A}_{d,n}|}{|\mathfrak{C}_{d,n}|} \leq 1 + C(p)^{n-1} D(p)^{n-2} p^{d_{n-1} - d_n/4 + d^2}.$$

The proof of Theorem 1.3 uses a theorem estimating the number of normal subgroups of an arbitrary finite p-group, applying it to quotients of free groups.

Theorem 1.4. *Fix a prime* p *and integers* d *and* n *so that either* $n = 2$ *and* $d \geq 10$ *or* $n \geq 3$ *and* $d \geq 3$. *Let* F *be the free group on* d *generators and let* d_n *be the rank of* F_n/F_{n+1}. *Let*

$$K = \begin{cases} C(p)^5 D(p)^4 p^{17/4} & : \quad n = 2 \text{ and } d \geq 10 \\ C(p)^2 D(p) p^{3/4} & : \quad n \geq 3. \end{cases}$$

Let

$$x = \begin{cases} -d & : \quad n = 2 \\ d^2 - d_n/2 & : \quad n \geq 3. \end{cases}$$

Then

(a)

$$1 \leq \frac{|\mathfrak{C}_{d,n}| \cdot |\mathrm{GL}(d, \mathbb{F}_p)|}{|\mathcal{C}_{d,n}|} \leq 1 + Kp^x.$$

(b)

$$1 \leq \frac{|\mathfrak{C}_{d,n}|}{|\mathfrak{D}_{d,n}|} \leq \frac{1 + Kp^x}{1 - Kp^x}.$$

In stating Theorems 1.3 and 1.4, we have judged it more satisfactory to give explicit numerical bounds, even though the proof of Theorem 1.1 requires only asymptotic bounds. However, since we have no expectation that our proof method gives bounds that are sharp, we have opted for clean explicit bounds rather than the best possible.

As we will show in Section 7, Theorem 1.1 follows easily from Theorems 1.2, 1.3, and 1.4. We close Section 7 with some observations and open questions.

2 The Lower p-Series

In this section, we define and discuss the *lower p-series* of a group (also called the *lower central p-series* or the *lower exponent-p central series*). Then, in Theorems 2.7 and 2.8, we describe how isomorphism classes of finite p-groups in a variety may be enumerated, obtaining Theorem 1.2 as a corollary.

2.1 Preliminaries

The lower p-series was introduced by Skopin [29] and Lazard [17], and it is described in detail by Huppert and Blackburn [16, Chapter VIII] (under the name λ-series) and by Bryant and Kovács [3]. The lower p-series is particularly suited to computer analysis of finite p-groups and forms the basis of the p-group generation algorithm of M. F. Newman [23] (this algorithm is described in greater detail in, for example, O'Brien [25]). This algorithm was modified in [26] and [4] to construct automorphism groups of finite p-groups. It should also be mentioned that some information about the lower p-series has appeared in [25] and [4], while the link between the lower p-series and automorphisms described in Subsection 2.2 is an extension of results that Higman [13] and Sims [28] used to count finite p-groups.

Definition. Fix a prime p. For any group H, the *lower p-series* $H = H_1 \geq H_2 \geq \cdots$ of H is defined by $H_{i+1} = H_i^p[H_i, H]$ for $i \geq 1$. H is said to have *lower p-length* n if H_n is the last non-identity element of the lower p-series.

Note that if H is a finite p-group, then $H_2 = \Phi(H)$, the Frattini subgroup of H. Before we list some basic facts about the lower p-series, recall that a subgroup is *fully invariant* if every endomorphism of the group restricts to an endomorphism of the subgroup. Also, we will write $H = \gamma_1(H) \geq \gamma_2(H) \geq \cdots$ to denote the *lower central series* of H, where $\gamma_{i+1}(H) = [\gamma_i(H), H]$. The

following proposition states five fundamental properties of the lower p-series; the first four facts are proved in Huppert and Blackburn [16, Chapter VIII, Theorem 1.5 and Corollary 1.6] and the fifth fact is obvious by induction.

Proposition 2.1. *For all positive integers i and j,*

1. $[H_i, H_j] \leq H_{i+j}$.
2. $H_i^{p^j} \leq H_{i+j}$.
3. $H_i = \gamma_1(H)^{p^{i-1}}\gamma_2(H)^{p^{i-2}} \cdots \gamma_i(H)$.
4. *H_{i+1} is the smallest normal subgroup of H lying in H_i such that H_i/H_{i+1} is an elementary abelian p-group and is central in H/H_{i+1}.*
5. *H_i is fully invariant in H.*

As we will see, the fact that H_i/H_{i+1} is elementary abelian, and therefore an $\mathbb{F}_p$-vector space, is a key reason we are able to prove the main theorem. It is easy to see the following proposition.

Proposition 2.2. *Let H be a finite group. Then H is a p-group if and only if H has finite lower p-length.*

The lower p-length of a finite p-group is related to the lower p-series of a free group in the following way. Let F be the free group on d generators; then any finite p-group H that is minimally d-generated is isomorphic to F/U for some normal subgroup U of F. By induction, $H_i = F_iU/U$:

$$\begin{aligned} H_{i+1} &= (F_iU/U)^p[F_iU/U, F/U] \\ &= F_i^p[F_i, F]U/U \\ &= F_{i+1}U/U. \end{aligned}$$

So the lower p-length of H is n, where F_{n+1} is the first term in the lower p-series of F that is contained in U.

2.2 The Lower p-Series and Automorphisms

In this subsection we collect some necessary facts linking the lower p-series and automorphisms. First, suppose that H is a finite p-group that is minimally d-generated. Of course, every automorphism of H induces an automorphism of H_i/H_{i+1} for each i. In particular, any automorphism of H induces an element of $\mathrm{Aut}(H/H_2) \cong \mathrm{GL}(d, \mathbb{F}_p)$ (by the Burnside Basis Theorem, the rank of H/H_2 is d). Thus we obtain a map from $\mathrm{Aut}(H)$ to $\mathrm{GL}(d, \mathbb{F}_p)$, and an exact sequence

$$1 \to K(H) \to \mathrm{Aut}(H) \to A(H) \to 1,$$

where $A(H)$ is a subgroup of $\mathrm{GL}(d, \mathbb{F}_p)$. The group $K(H)$ acts trivially on H/H_2, and hence on each factor H_i/H_{i+1} (see Huppert and Blackburn [16, Chapter VIII, Theorem 1.7]). As $\mathrm{Aut}(H)$ acts on each H_i/H_{i+1} and the kernel of the action contains $K(H)$, we obtain an action of $A(H)$ on each H_i/H_{i+1}. The following key proposition is due to P. Hall [10, Section 1.3].

Proposition 2.3. *If H is a finite p-group, then so is $K(H)$.*

Let F be the free group on d generators $y_1, y_2, \ldots, y_d$. We need two observations about the subgroup F_2, first recalling an obvious result on the Frattini quotient.

Proposition 2.4. *If H is a finite p-group and θ is an endomorphism of H that induces an automorphism on the Frattini quotient H/H_2, then θ is an automorphism of H.*

Proposition 2.5. *F_2 is a maximal fully invariant subgroup of F.*

Proof. Suppose $U > F_2$ is a fully invariant subgroup of F. The elements $y_1^{a_1} \cdots y_d^{a_d}$, with $0 \leq a_i < p$, form a complete set of coset representatives for the cosets of F_2 in F, so U contains an element $y = y_1^{a_1} \cdots y_d^{a_d}$ with some a_i nonzero. Fix $1 \leq k \leq d$ and let b_i be a multiplicative inverse of a_i modulo p. Then the endomorphism of F that sends y_j to 1 for $j \neq i$ and sends y_i to $y_k^{b_i}$ also sends y to y_k, showing that $y_k \in U$. This holds for $1 \leq k \leq d$, and so $U = F$. □

Proposition 2.6. *Let U be a fully invariant subgroup of F contained in F_2 with $H = F/U$ a finite p-group. Then any automorphism θ of F/F_2 lifts to an automorphism of H.*

Proof. Since F is free, there is an endomorphism θ' of F such that $\theta'(y_i) \in \theta(y_i F_2)$ for $1 \leq i \leq d$. Therefore $\theta'(y) \in \theta(yF_2)$ for all $y \in F$. Then θ' induces θ on F/F_2, and since U is fully invariant, maps U to itself. So θ' induces an endomorphism θ'' of H. But θ'' induces θ, an automorphism of $F/F_2 \cong (F/U)/(F_2/U) \cong H/H_2$, the Frattini quotient of H. By Proposition 2.4, θ'' is an automorphism of H. Thus θ lifts to an automorphism θ'' of H. □

Finally, we note that by Huppert and Blackburn [16, Chapter VIII, Theorem 11.15], the rank of $F/[F,F]$, and hence of F/F_2, is d, and the rank of F_n/F_{n+1} is finite for each n (in Section 3, we will compute the rank of F_n/F_{n+1} in general).

2.3 Enumerating Groups in a Variety

A *variety of groups* V consists of all groups G satisfying a set of relations $w = 1$, where w ranges over a fixed set W of group words (see Neumann [22]). Let F be the free group on d generators. The variety V contains a *relatively free group* on d generators, namely F/U, where U is the *verbal subgroup* of F generated by all the values of $w \in W$. For example, all abelian groups form the variety in which the relation $ab = ba$ holds for all group elements a and b. Then the free abelian group on d generators is the relatively free group on d generators in the variety of abelian groups. We will only be interested in the variety of p-groups of lower p-length at most n, but the theorems in this subsection hold in more general situations.

Let U be a fully invariant subgroup of F. Then $G = F/U$ is a relatively free group in some variety V on at most d generators. The relations defining

V come from setting each word in U equal to the identity element. Suppose that G is a finite non-trivial p-group. In this setting, we can describe $A(G)$ and $K(G)$ more precisely.

Note that F_2U is a fully invariant subgroup of F, and by Proposition 2.5, either $F = F_2U$ or $F_2 = F_2U$. In the first case, $F = U$, contradicting the non-triviality of G. Thus $F_2 = F_2U$ and $U \leq F_2$. Since F/F_2 has rank d, both F and F/F_2 are minimally generated by d elements. It follows that $G = F/U$ is also minimally generated by d elements.

Theorem 2.7. *Suppose that G is the relatively free group on d generators in a variety of groups V and that $|G| = p^g$. Then*

$$1 \to K(G) \to \mathrm{Aut}(G) \to \mathrm{GL}(d, \mathbb{F}_p) \to 1$$

is exact and $|K(G)| = p^{d(g-d)}$. Furthermore, the map $L \mapsto G/L$ defines a bijection between $\mathrm{Aut}(G)$-orbits of normal subgroups L of G lying in G_2 and d-generator groups in V. If $H = G/L$, then

$$1 \to B(L) \to N_{\mathrm{Aut}(G)}(L) \to \mathrm{Aut}(H) \to 1$$

is exact, where $B(L)$ is the subgroup of $N_{\mathrm{Aut}(G)}(L)$ that acts trivially on H. If $|L| = p^m$, then $|B(L)| = p^{dm}$.

Proof. By Proposition 2.6, any automorphism θ of $F/F_2 \cong G/G_2$ lifts to an automorphism of G. Thus $A(G)$ is the full automorphism group of F/F_2, which is $\mathrm{GL}(d, \mathbb{F}_p)$. This proves that $1 \to K(G) \to \mathrm{Aut}(G) \to \mathrm{GL}(d, \mathbb{F}_p) \to 1$ is exact.

Let $x_1, \ldots, x_d$ be a minimal generating set for G. Also let L be a normal subgroup of G lying in G_2 and let $u_1, \ldots, u_d$ be any elements of L. Since G is relatively free, the map $\alpha : x_i \mapsto x_i u_i$ for each i is an endomorphism of G (it suffices to check that if a word w in the x_i's equals 1, then $w\alpha = 1$, but every tuple of elements of G satisfies the same relations, so when x_i is replaced by $x_i u_i$ in w, the new word also equals 1). Furthermore, α acts trivially on G/L and is an automorphism by Proposition 2.4. Conversely, any automorphism of G that acts trivially on G/L must act on each x_i as multiplication by an element of L. Thus the number of automorphisms of G that act trivially on G/L is $|L|^d$. Taking $L = G_2$ gives $|K(G)| = p^{d(g-d)}$.

Next, we claim that any group H in V that is minimally generated by d elements is isomorphic to G/L for some normal subgroup L of G lying in G_2. Evidently H is isomorphic to G/L for some normal subgroup L of G; it suffices to show that if $L \not\leq G_2$, then G/L will be generated by fewer than d elements. Choose $x_1 \in L \setminus G_2$. Extend $\{x_1\}$ to a generating set $\{x_1, \ldots, x_d\}$ of G. Then G/L is generated by the images of $\{x_2, \ldots, x_d\}$.

Suppose M is a normal subgroup of G in the same $\mathrm{Aut}(G)$-orbit as L. Clearly $G/M \cong G/L$, so the map $L \mapsto G/L$ is well-defined on $\mathrm{Aut}(G)$-orbits of normal subgroups of G lying in G_2. To show that this is a bijection, we must show that if M is a normal subgroup of G lying in G_2 with $G/M \cong G/L$, then M is in the same $\mathrm{Aut}(G)$-orbit as L. Let $\beta : G/L \to G/M$ be an isomorphism. By [22,

Theorem 44.21], G is projective, as in [22, Definition 44.11]; as the quotient map from G to G/M is surjective, this says that there exists an endomorphism $\gamma : G \to G$ so that the diagram in Figure 1 commutes. Then γ induces β, and β induces an automorphism on the Frattini quotient of G (since the Frattini quotients of G/L and G/M are isomorphic to the Frattini quotient of G). It follows from Proposition 2.4 that γ is an automorphism of G. From Figure 1, it is also clear that $L\gamma \leq M$. Thus $L\gamma = M$, and L and M are in the same $\mathrm{Aut}(G)$-orbit.

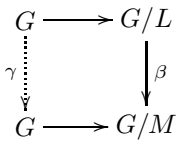


Figure 1

If we take $L = M$, we find that any automorphism of $H = G/L$ is induced by an automorphism of G, so that $\mathrm{Aut}(H) \cong N_{\mathrm{Aut}(G)}(L)/B(L)$, where $B(L)$ is the subgroup of $N_{\mathrm{Aut}(G)}(L)$ that acts trivially on H. By the earlier argument in this proof, $|B(L)| = |L|^d$. □

Theorem 2.8. *Suppose that G is the relatively free group on d generators in a variety of groups V and suppose that G has lower p-length n. The map $L \mapsto G/L$ defines a bijection between $\mathrm{GL}(d, \mathbb{F}_p)$-orbits on normal subgroups L of G lying in G_n and groups H in V that are minimally generated by d elements and satisfy $H/H_n \cong G/G_n$. If $H = G/L$, then*

$$1 \to K(G)/B(L) \to \mathrm{Aut}(H) \to N_{\mathrm{GL}(d,\mathbb{F}_p)}(L) \to 1$$

is exact, where $B(L)$ is the subgroup of $N_{\mathrm{Aut}(G)}(L)$ that acts trivially on H. Moreover, $K(H)$ is the image of $K(G)/B(L)$ in $\mathrm{Aut}(H)$.

Proof. $H/H_n \cong G/G_nL$ is isomorphic to G/G_n if and only if $L \leq G_n$. Furthermore, $K(G)$ acts trivially on $G_n \cong G_n/G_{n+1}$ as noted in Subsection 2.2, so the $\mathrm{Aut}(G)$-orbits of normal subgroups of G lying in G_n are just the $\mathrm{GL}(d, \mathbb{F}_p)$-orbits. This proves the bijection.

Since $K(G)$ fixes L, it also follows that

$$1 \to K(G) \to N_{\mathrm{Aut}(G)}(L) \to N_{\mathrm{GL}(d,\mathbb{F}_p)}(L) \to 1$$

is exact. Combined with the second exact sequence in Theorem 2.7, we find that

$$1 \to K(G)/B(L) \to \mathrm{Aut}(H) \to N_{\mathrm{GL}(d,\mathbb{F}_p)}(L) \to 1$$

is exact. Every automorphism in $K(G)$ induces an automorphism in $K(H)$ since $K(G)$ fixes L and $G/G_2 \cong H/H_2$. Conversely, every automorphism in $K(H)$ is induced by an automorphism in $K(G)$. The kernel of the map from $K(G)$ to $K(H)$ is $B(L)$, so $K(H)$ is the image of $K(G)/B(L)$. □

We can now prove Theorem 1.2, restated here for convenience.

Theorem 1.2. *Fix a prime p and integers $d, n \geq 2$. Let F be the free group on d generators and define the following sets:*

$$\begin{aligned}
\mathcal{A}_{d,n} &= \{\textit{normal subgroups of } F/F_{n+1} \textit{ lying in } F_2/F_{n+1}\} \\
\mathcal{B}_{d,n} &= \{\textit{normal subgroups of } F/F_{n+1} \textit{ lying in } F_2/F_{n+1} \\
&\qquad \textit{and not containing } F_n/F_{n+1}\} \\
\mathcal{C}_{d,n} &= \{\textit{normal subgroups of } F/F_{n+1} \textit{ lying in } F_n/F_{n+1}\} \\
\mathcal{D}_{d,n} &= \{\textit{normal subgroups of } F/F_{n+1} \textit{ contained in the} \\
&\qquad \textit{regular } \mathrm{GL}(d,\mathbb{F}_p)\textit{-orbits in } \mathfrak{C}_{d,n}\}
\end{aligned}$$

$$\begin{aligned}
\mathfrak{A}_{d,n} &= \{\mathrm{Aut}(F/F_{n+1})\textit{-orbits in } \mathcal{A}_{d,n}\} \\
\mathfrak{B}_{d,n} &= \{\mathrm{Aut}(F/F_{n+1})\textit{-orbits in } \mathcal{B}_{d,n}\} \\
\mathfrak{C}_{d,n} &= \{\mathrm{Aut}(F/F_{n+1})\textit{-orbits in } \mathcal{C}_{d,n}\} = \{\mathrm{GL}(d,\mathbb{F}_p)\textit{-orbits in } \mathcal{C}_{d,n}\} \\
\mathfrak{D}_{d,n} &= \{\textit{regular } \mathrm{GL}(d,\mathbb{F}_p)\textit{-orbits in } \mathcal{C}_{d,n}\}.
\end{aligned}$$

Then there is a well-defined map $\pi_{d,n} : \mathfrak{A}_{d,n} \to \{$finite p-groups$\}$ given by $L/F_{n+1} \mapsto F/L$, where $L/F_{n+1} \in \mathcal{A}_{d,n}$. Furthermore $\pi_{d,n}$ induces bijections

$$\begin{aligned}
\mathfrak{A}_{d,n} &\leftrightarrow \{p\textit{-groups of lower } p\textit{-length at most } n \\
&\qquad \textit{and minimally generated by } d \textit{ elements}\} \\
\mathfrak{B}_{d,n} &\leftrightarrow \{p\textit{-groups of lower } p\textit{-length } n \\
&\qquad \textit{and minimally generated by } d \textit{ elements}\} \\
\mathfrak{D}_{d,n} &\leftrightarrow \{\textit{subgroups } H \textit{ in } \pi_{d,n}(\mathfrak{C}_{d,n}) \textit{ with } A(H) = 1\}.
\end{aligned}$$

Proof. Take V to be the variety of p-groups of lower p-length at most n. Then F/F_{n+1} is the relatively free group on d generators in V. The $\mathrm{Aut}(F/F_{n+1})$- and $\mathrm{GL}(d,\mathbb{F}_p)$-orbits in $\mathcal{C}_{d,n}$ are the same because of the first exact sequence in Theorem 2.7 and the fact that $K(F/F_{n+1})$ acts trivially on F_n/F_{n+1} as in Subsection 2.2.

The map $\pi_{d,n}$ is well-defined and defines bijections for $\mathfrak{A}_{d,n}$ and $\mathfrak{B}_{d,n}$ by Theorem 2.7. A normal subgroup L of F/F_{n+1} lying in F_n/F_{n+1} is in a regular $\mathrm{GL}(d,\mathbb{F}_p)$-orbit if $N_{\mathrm{GL}(d,\mathbb{F}_p)}(L) = 1$. By Theorem 2.8, L is in a regular orbit if and only if $A(H) = 1$. Thus the bijection for $\mathfrak{D}_{d,n}$ is proved. □

Note, by the way, that since F_n/F_{n+1} is elementary abelian and central in F/F_{n+1}, the set $\mathcal{C}_{d,n}$ is just the set of subspaces of the vector space F_n/F_{n+1}.

3 The Lower p-Series of a Free Group

Let F be the free group on d generators $y_1, y_2, \ldots, y_d$. To prepare for Sections 5 and 6, we need to analyze the $\mathbb{F}_p\mathrm{GL}(d,\mathbb{F}_p)$-module structure of F_n/F_{n+1} along with power and commutator maps from F_n/F_{n+1} to F_{n+1}/F_{n+2}. Our main tool

will be the connection between the lower p-series of F and the free Lie algebra described in Theorem 3.2. The results of Theorem 3.2 appear several times in the literature with varying degrees of correctness and detail. Our presentation follows Bryant and Kovács [3], while the most complete proofs may be inferred from Huppert and Blackburn [16, Chapter VIII]. Information about the free Lie algebra can be found in Garsia [7] and Reutenauer [27].

Let K be any field and let $A = \{x_1, \ldots, x_d\}$ be an alphabet on d letters. Write A^* for the collection of all A-words and A^n for the collection of all A-words of length n. Let $K[A^*]$ denote the free associative K-algebra on the generators $x_1, x_2, \ldots, x_d$; equivalently, $K[A^*]$ is the non-commutative algebra of polynomials

$$f = \sum_{w \in A^*} f_w w$$

with coefficients $f_w \in K$. The algebra $K[A^*]$ is graded by degree; let $K[A^n]$ denote the homogeneous component of degree n. Also, $K[A^*]$ is a Lie algebra under the Lie bracket $[f, g] = fg - gf$. Let $K[\Lambda^*]$ denote the Lie subalgebra of $K[A^*]$ generated by $x_1, \ldots, x_d$ and the Lie bracket. Then $K[\Lambda^*]$ is the *free Lie algebra* over K on $x_1, \ldots, x_d$. It is also graded by degree; let $K[\Lambda^n]$ be the homogeneous component of $K[\Lambda^*]$ of degree n.

It will be convenient to specify a basis of $K[\Lambda^n]$. Lexicographically order the set A^*, where $x_1 < x_2 < \cdots < x_d$. A word w is a *Lyndon word* if it is smaller than all of its proper non-trivial tails. Let L be the set of Lyndon words, and let L_n be the set of Lyndon words of length n. Inductively define the *right standard bracketing* $b[w]$ of $w \in L$ by

$$b[w] = w$$

if $w \in A$ and otherwise by

$$b[w] = [b[w_1], b[w_2]],$$

where $w = w_1 w_2$ and w_2 is the longest proper tail of w that is a Lyndon word.

Theorem 3.1 (Reutenauer [27, Proof of Theorem 5.1]). *If $w \in L$, then*

$$b[w] = w + \sum_{w < v} f_v v$$

for some $f_v \in K$. The set $\{b[w] : w \in L_n\}$ forms a basis for $K[\Lambda^n]$.

The results in this section require many maps; in an attempt to clarify matters, we will define all the maps now, using suggestive names, and postpone stating their properties until necessary.

Definition. Fix a prime p. Fix integers $n \geq 1$, $d \geq 2$, and $1 \leq j \leq d$. Let $f_i \in F_i$ for each $i \geq 1$.

- $\mathrm{pow}_n : F_n/F_{n+1} \to F_{n+1}/F_{n+2}$
  (*a power map on F*)
  $\mathrm{pow}_n : f_n F_{n+1} \quad \mapsto \quad f_n^p F_{n+2}$

- $\mathrm{Fcom}_{j,n} : F_n/F_{n+1} \to F_{n+1}/F_{n+2}$
  (*a commutator map on* F)
  $\mathrm{Fcom}_{j,n} : f_n F_{n+1} \quad \mapsto \quad [f_n, y_j]F_{n+2}$
- $\mathrm{emb}_n : F_n \to \mathbb{F}_p[A^*]$
  (*an embedding of* F_n *into* $\mathbb{F}_p[A^*]$)
  $$\begin{array}{lll} \mathrm{emb}_1 : & y_j & \mapsto \quad x_j \\ \mathrm{emb}_n : & f_{n-1}^p & \mapsto \quad \begin{cases} \mathrm{emb}_1(f_1) + \mathrm{emb}_1(f_1)^2 : n = 2 \text{ and } p = 2 \\ \mathrm{emb}_{n-1}(f_{n-1}) \quad : \text{otherwise} \end{cases} \\ \mathrm{emb}_n : & [f_{n-1}, f_1] & \mapsto \quad [\mathrm{emb}_{n-1}(f_{n-1}), \mathrm{emb}_1(f_1)] \\ \mathrm{emb}_n : & f_{n+1} & \mapsto \quad 0 \end{array}$$
- $\mathrm{qemb}_n : F_n/F_{n+1} \to \mathbb{F}_p[A^*]$
  (*an embedding of the quotient* F_n/F_{n+1} *into* $\mathbb{F}_p[A^*]$)
  qemb_n is induced by emb_n
- $\mathrm{com} : \{\text{subspaces of } \mathbb{F}_p[A^*]\} \to \{\text{subspaces of } \mathbb{F}_p[A^*]\}$
  (*a commutator map on* $\mathbb{F}_p[A^*]$)
  $\mathrm{com} : W \quad \mapsto \quad [W, \mathbb{F}_p[\Lambda^1]]$
- $\mathrm{com}_j : \mathbb{F}_p[A^*] \to \mathbb{F}_p[A^*]$
  (*a commutator map on* $\mathbb{F}_p[A^*]$)
  $\mathrm{com}_j : f \quad \mapsto \quad [f, x_j]$
- $\mathrm{com}_{j,n} : \mathbb{F}_p[A^n] \to \mathbb{F}_p[A^{n+1}]$
  (*a commutator map on* $\mathbb{F}_p[A^n]$)
  $\mathrm{com}_{j,n}$ is induced by com_j.
- $\mathrm{proj}_n : \mathbb{F}_p[A^*] \to \mathbb{F}_p[A^n]$
  (*the projection map onto* $\mathbb{F}_p[A^n]$)

Theorem 3.2. *The map* emb_n *is a well-defined homomorphism. The map* qemb_n *is an* $\mathbb{F}_p\mathrm{GL}(d, \mathbb{F}_p)$*-module embedding of* F_n/F_{n+1} *into* $\mathbb{F}_p[A^*]$*. If* p *is odd, the image of* qemb_n *is* $\mathbb{F}_p[\Lambda^1] \oplus \cdots \oplus \mathbb{F}_p[\Lambda^n]$*, and hence*

$$F_n/F_{n+1} \cong \mathbb{F}_p[\Lambda^1] \oplus \cdots \oplus \mathbb{F}_p[\Lambda^n]$$

as $\mathbb{F}_p\mathrm{GL}(d, \mathbb{F}_p)$*-modules.*

If $p = 2$*, the image of* qemb_1 *is* $\mathbb{F}_2[\Lambda^1]$*. The image* E *of* qemb_2 *satisfies*

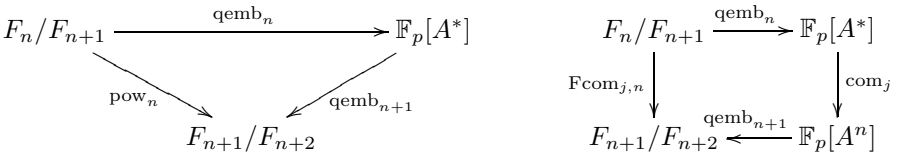
$$E + \mathbb{F}_2[A^2] = \mathbb{F}_2[A^1] \oplus \mathbb{F}_2[A^2] \quad \textit{and} \quad E \cap \mathbb{F}_2[A^2] = \mathbb{F}_2[\Lambda^2],$$

so E *is an extension of* $\mathbb{F}_2[\Lambda^2]$ *by* $\mathbb{F}_2[\Lambda^1]$*. For* $n \geq 3$*, the image of* qemb_n *is* $E \oplus \mathbb{F}_2[\Lambda^3] \oplus \cdots \oplus \mathbb{F}_2[\Lambda^n]$*, and hence*

$$F_n/F_{n+1} \cong E \oplus \mathbb{F}_2[\Lambda^3] \oplus \cdots \oplus \mathbb{F}_2[\Lambda^n].$$

Note that as a $\mathbb{F}_p\mathrm{GL}(d,\mathbb{F}_p)$-module, $\mathbb{F}_p[\Lambda^n] \cong V \wedge V \wedge \cdots \wedge V$, the n-fold wedge product where V is the natural $\mathbb{F}_p\mathrm{GL}(d,\mathbb{F}_p)$-module.

Corollary 3.3. *Unless $p = 2$ and $n = 1$, the diagram on the left commutes and pow_n is an injective homomorphism. The diagram on the right commutes and $\mathrm{Fcom}_{j,n}$ is a homomorphism.*



The dimension of $K[\Lambda^i]$ is given by Witt's formula:

$$\dim(K[\Lambda^i]) = \frac{1}{i}\sum_{j|i} \mu(i/j) \cdot d^j,$$

where μ is the Möbius function (see [27, Appendix 0.4.2]). Thus Theorem 3.2 tells us the rank of F_n/F_{n+1}.

Corollary 3.4. *The rank of F_n/F_{n+1} is*

$$\sum_{i=1}^{n} \frac{1}{i}\sum_{j|i} \mu(i/j) \cdot d^j.$$

The remainder of this section is devoted to proving the following theorem and corollary. Corollary 3.6 will allow us to count normal subgroups of F/F_{n+1} when combined with Theorem 5.1.

Theorem 3.5. *Fix a prime p and integers $d \geq 3$ and $n \geq 2$. Suppose that U is a normal subgroup of F lying in F_2. Let*

$$\begin{aligned} Q &= (U \cap F_n)F_{n+1}/F_{n+1} \\ R &= (U_2 \cap F_{n+1})F_{n+2}/F_{n+2} \\ S &= (U^p[U,F] \cap F_{n+1})F_{n+2}/F_{n+2}. \end{aligned}$$

Then $\mathrm{rank}(R) \geq \mathrm{rank}(Q)$ *and* $\mathrm{rank}(S) \geq (3/2)\,\mathrm{rank}(Q)$.

The third isomorphism theorem lets us replace F by F/F_n, giving the following corollary.

Corollary 3.6. *Fix a prime p and integers $d \geq 3$, $n \geq 3$, and $2 \leq i < n$. Let $G = F/F_{n+1}$. Suppose that U is a normal subgroup of G lying in G_2. Let*

$$\begin{aligned} Q &= (U \cap G_i)G_{i+1}/G_{i+1} \\ R &= (U_2 \cap G_{i+1})G_{i+2}/G_{i+2} \\ S &= (U^p[U,F] \cap G_{i+1})G_{i+2}/G_{i+2}. \end{aligned}$$

Then $\mathrm{rank}(R) \geq \mathrm{rank}(Q)$ *and* $\mathrm{rank}(S) \geq (3/2)\,\mathrm{rank}(Q)$.

To prove Theorem 3.5, we will build up to an analogous result for the free Lie algebra on d generators (Lemma 3.11) and then apply Theorem 3.2.

Lemma 3.7. *The following diagram commutes:*

$$\begin{array}{ccc} \mathbb{F}_p[A^*] & \xrightarrow{\mathrm{com}_j} & \mathbb{F}_p[A^*] \\ \downarrow{\scriptstyle \mathrm{proj}_n} & & \downarrow{\scriptstyle \mathrm{proj}_{n+1}} \\ \mathbb{F}_p[A^n] & \xrightarrow[\mathrm{com}_{j,n}]{} & \mathbb{F}_p[A^{n+1}] \end{array}$$

If $n = 1$, then the kernel of $\mathrm{com}_{j,n}$ is spanned by x_j. If $n > 1$, then $\mathrm{com}_{j,n}$ is injective.

Proof. The only statements requiring proof are those about the kernel and injectivity of $\mathrm{com}_{j,n}$. Without loss of generality, we may assume that $j = 1$. Suppose that $w \in L_n$. Unless $n = 1$ and $w = x_1$, we see that $x_1 w$ is smaller than w, and hence smaller than all of its proper non-trivial tails. So $x_1 w \in L_{n+1}$. Furthermore, w is the longest tail of $x_1 w$ that is a Lyndon word, so $b[x_1 w] = -[b[w], x_1]$. Thus the image of $b[w]$ under $\mathrm{com}_{1,n}$ is the negative of a basis element in L_{n+1}, unique for each w. It follows that the kernel of $\mathrm{com}_{1,1}$ is generated by x_1 and $\mathrm{com}_{1,n}$ is injective for $n > 1$. □

Lemma 3.8. *Fix $d \geq 3$ and $n \geq 2$. Suppose that W is a subspace of $\mathbb{F}_p[\Lambda^n]$. Then $\dim(\mathrm{com}(W)) \geq (3/2)\dim(W)$.*

Proof. Let $\mathbb{F}_p[\Lambda^*]_{ij}$ denote the free Lie algebra on two generators x_i and x_j; there is a natural embedding of $\mathbb{F}_p[\Lambda^*]_{ij}$ into $\mathbb{F}_p[\Lambda^*]$. Let $\mathbb{F}_p[\Lambda^n]_{ij}$ be the homogeneous component of degree n in $\mathbb{F}_p[\Lambda^*]_{ij}$.

First, we claim that if f and g are distinct elements of $\mathbb{F}_p[\Lambda^n]$ and $[f, x_i] = [g, x_j]$, then in fact $f, g \in \mathbb{F}_p[\Lambda^n]_{ij}$. We may assume that $i, j > 1$. Suppose that $f \notin \mathbb{F}_p[\Lambda^n]_{ij}$. Then writing

$$f = \sum_{w \in L_n} f_w b[w],$$

there must be some word $w \in L_n$ where $f_w \neq 0$ and w contains a letter other than x_i and x_j. We may assume that w contains the letter x_1. In that case, by Theorem 3.1, there is a word beginning with x_1 that appears in f with non-zero coefficient. Thus there is a word beginning with x_1 and ending with x_i that appears in $[f, x_i]$ with non-zero coefficient. No such word can appear in $[g, x_j]$, contradicting the fact that $[f, x_i] = [g, x_j]$. Hence $f \in \mathbb{F}_p[\Lambda^n]_{ij}$ and similarly $g \in \mathbb{F}_p[\Lambda^n]_{ij}$.

Note that $\mathbb{F}_p[\Lambda^n]_{ij} \cap \mathbb{F}_p[\Lambda^n]_{kl} = 0$ if $\{i, j\} \neq \{k, l\}$ (the letters x_i and x_j appear in every element of $\mathbb{F}_p[\Lambda^n]_{ij}$ since $n > 1$). Choose i and j so that $\dim(W \cap \mathbb{F}_p[\Lambda^n]_{ij})$ is as small as possible; in particular this intersection has dimension at most $(1/2)\dim(W)$. Let X be a complement to $W \cap \mathbb{F}_p[\Lambda^n]_{ij}$ in W.

Define a more restrictive commutator map on subspaces by $\mathrm{com}_{ij} : \bullet \mapsto [\bullet, \mathbb{F}_p[\Lambda^1]_{ij}]$. Obviously $\mathrm{com}_{ij}(W) \subseteq \mathrm{com}(W)$. Using Lemma 3.7 and the above claim,

$$\begin{aligned}\dim(\mathrm{com}_{ij}(W)) &= \dim(\mathrm{com}_{ij}(W \cap \mathbb{F}_p[\Lambda^n]_{ij})) + \dim(\mathrm{com}_{ij}(X)) \\ &\geq \dim(W \cap \mathbb{F}_p[\Lambda^n]_{ij}) + 2\dim(X) \\ &\geq (3/2)\dim W.\end{aligned}$$

□

Lemma 3.9. *Fix $d \geq 2$. Suppose that W be a subspace of $\mathbb{F}_p[\Lambda^1]$. Then* $\dim(W + \mathrm{com}(W)) \geq (3/2)\dim(W)$.

Proof. Recalling Lemma 3.7, this is clear if $\dim(W) = 1$, and otherwise

$$\dim(\mathrm{com}_{1,1}(W)) \geq \dim(W) - 1,$$

implying the result since W and $\mathrm{com}(W)$ are disjoint. □

Lemma 3.10. *Let $p = 2$. Suppose that W is a subspace of E, where E is defined in Theorem 3.2. Then* $\dim(W + \mathrm{com}(W)) \geq (3/2)\dim(W)$.

Proof. Let $X = W \cap \mathbb{F}_2[\Lambda^2]$ and let Y be a complement to X in W. Note that $\dim(Y) = \dim(\mathrm{proj}_1(Y))$. By Lemma 3.9,

$$\dim(\mathrm{proj}_1(Y) + \mathrm{com}(\mathrm{proj}_1(Y))) \geq (3/2)\dim(\mathrm{proj}_1(Y)).$$

By the commutative diagram in Lemma 3.7, it follows that $Y + \mathrm{com}(Y)$ contains a subspace of dimension at least $(3/2)\dim(Y)$ that has trivial intersection with $\mathbb{F}_2[\Lambda^3]$. By Lemma 3.8, $\mathrm{com}(X) \leq \mathbb{F}_2[\Lambda^3]$ contains a subspace of dimension at least $(3/2)\dim(X)$. Then

$$\dim(W + \mathrm{com}(W)) \geq (3/2)\dim(X) + (3/2)\dim(Y) = (3/2)\dim(W).$$

□

Lemma 3.11. *Fix $d \geq 3$. Let $U_n = \mathbb{F}_p[\Lambda^1] \oplus \cdots \oplus \mathbb{F}_p[\Lambda^n]$ if p is odd or $U_n = E \oplus \mathbb{F}_2[\Lambda^3] \oplus \cdots \oplus \mathbb{F}_2[\Lambda^n]$ if $p = 2$. Suppose that W is a subspace of $\mathbb{F}_p[A^*]$ contained in U_n. Then* $\dim(W + \mathrm{com}(W)) \geq (3/2)\dim(W)$.

Proof. The proof will be by induction on n. When p is odd and $n = 1$, Lemma 3.9 gives the result. When $p = 2$ and $n = 2$, Lemma 3.10 gives the result. So assume that p is odd and $n > 1$ or that $p = 2$ and $n > 2$. Assume the result holds for $n - 1$. Let $X = W \cap U_{n-1}$. By the inductive hypothesis,

$$\dim(X + \mathrm{com}(X)) \geq (3/2)\dim(X).$$

Furthermore, $X + \mathrm{com}(X) \leq U_n$. Let Y be a complement to X in W. By the commutative diagram in Lemma 3.7, $\mathrm{com}(\mathrm{proj}_n(Y)) = \mathrm{proj}_{n+1}(\mathrm{com}(Y))$. By the definition of X and Y, $\dim(\mathrm{proj}_n(Y)) = \dim(Y)$. By Lemma 3.8,

$$\dim(\mathrm{proj}_{n+1}(\mathrm{com}(Y))) \geq (3/2)\dim(\mathrm{proj}_n(Y)).$$

Thus $\mathrm{com}(Y)$ contains a subspace of dimension at least $(3/2)\dim(\mathrm{proj}_n(Y))$ that has trivial intersection with U_n. Therefore

$$\dim(W + \mathrm{com}(W)) \geq (3/2)\dim(X) + (3/2)\dim(Y) = (3/2)\dim(W).$$

□

Proof of Theorem 3.5. Replacing U by $(U \cap F_n)F_{n+1}$ does not change Q, R, or S, so we may assume that $F_{n+1} \leq U \leq F_n$. Recall that by Corollary 3.3, pow_n is injective. Since $\mathrm{pow}_n(Q) = R$, it follows that $\mathrm{rank}(R) \geq \mathrm{rank}(Q)$.

Also by Corollary 3.3,

$$S = \mathrm{qemb}_{n+1}^{-1}(\mathrm{qemb}_n(U) + (\mathrm{com} \circ \mathrm{qemb}_n)(U)).$$

Since qemb_n is injective, and

$$\dim(\mathrm{qemb}_n(U) + (\mathrm{com} \circ \mathrm{qemb}_n)(U)) \geq (3/2)\dim(\mathrm{qemb}_n(U))$$

by Lemma 3.11, it follows that $\mathrm{rank}(S) \geq (3/2)\,\mathrm{rank}(Q)$. □

4 Numerical Estimates

The purpose of this section is to prove several estimates needed in Sections 5 and 6. Most of the estimates involve Gaussian coefficients, and so we will begin with the relevant definitions and bounds on the Gaussian coefficients obtained by Wilf [32].

The *Gaussian coefficient* (also called the *q-binomial coefficient*)

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n - 1)\cdots(q^n - q^{k-1})}{(q^k - 1)\cdots(q^k - q^{k-1})}$$

is the number of k-dimensional subspaces of a vector space of dimension n over $\mathbb{F}_q$. We shall be concerned with estimates for $\begin{bmatrix} n \\ k \end{bmatrix}_q$ and for the *Galois number*

$$\mathcal{G}_n(q) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q,$$

which is the total number of subspaces of a vector space of dimension n over $\mathbb{F}_q$. (A survey of these numbers is given by Goldman and Rota [9].) First we need a technical lemma.

Lemma 4.1. *Let*

$$C(q) = \sum_{r=-\infty}^{\infty} q^{-r^2}.$$

Let $f(x) = -ax^2 + bx + c$ with $a > 0$, let $|q| > 1$, and set $A(q) = \sum_r q^{f(r)}$, where the sum is over all integers r with $t \leq r \leq u$. Then $A(q) \leq C(q^a)q^{f(y)}$ for some $y \in [t, u]$.

Proof. Suppose the maximum of $f(x)$ in $[t,u]$ occurs at $x=y$. The global maximum of $f(x)$ occurs at $x=b/2a$, so one of three cases holds: $b/2a \le y = t$, $u = y \le b/2a$, or $t \le y = b/2a = u$. In each case, for all $r \in [t,u]$,

$$\begin{aligned} & -a(r-y)^2 - f(r) + f(y) \\ = \; & -a(r-y)^2 - (-ar^2+br+c) + (-ay^2+by+c) \\ = \; & (2ay-b)(r-y) \\ \ge \; & 0. \end{aligned}$$

Thus

$$\begin{aligned} A(q) &= q^{f(y)} \sum_{t \le r \le u} q^{f(r)-f(y)} \\ &\le q^{f(y)} \sum_{t \le r \le u} q^{-a(r-y)^2} \\ &\le q^{f(y)} \sum_{r=-\infty}^{\infty} q^{-a(r-y)^2}, \end{aligned}$$

and it suffices to show that

$$g(y) = \sum_{r=-\infty}^{\infty} s^{-(r-y)^2} \le g(0),$$

where $s = q^a$. This is a consequence of Jacobi's functional equation for the theta function

$$\theta_3(z,w) = \sum_{r=-\infty}^{\infty} e^{r^2 \pi i w} e^{2riz},$$

where $|e^{\pi i w}| < 1$. Section 21.51 of Whittaker and Watson [31] gives the functional equation

$$\theta_3(z,w) = \frac{1}{\sqrt{-iw}} e^{z^2/\pi i w} \theta_3(z/w, -1/w),$$

where $\sqrt{e^{i\theta}}$ denotes $e^{i\theta/2}$ for $0 \le \theta \le 2\pi$. Now

$$\begin{aligned} g(y) &= s^{-y^2} \sum_{r=-\infty}^{\infty} s^{-r^2} e^{-2ri(iy \log s)} \\ &= s^{-y^2} \theta_3(-iy \log s, w), \end{aligned}$$

where $s^{-1} = e^{\pi i w}$ so that $\pi i w = -\log s$. Hence

$$\begin{aligned} g(y) &= \frac{s^{-y^2}\sqrt{\pi}}{\sqrt{\log s}} e^{y^2 \log s} \theta_3(-\pi y, -1/w) \\ &= \sqrt{\frac{\pi}{\log s}} \sum_{r=-\infty}^{r=\infty} e^{-r^2\pi^2/\log s} e^{-2ir\pi y} \\ &= \sqrt{\frac{\pi}{\log s}} (1 + 2\sum_{r=1}^{\infty} e^{-r^2\pi^2/\log s} \cos 2r\pi y) \\ &\le \sqrt{\frac{\pi}{\log s}} (1 + 2\sum_{r=1}^{\infty} e^{-r^2\pi^2/\log s}) \\ &= g(0). \end{aligned}$$

□

To obtain bounds for Gaussian coefficients, let

$$\begin{aligned} D(q) &= \prod_{j=1}^{\infty} (1 - q^{-j})^{-1} \\ S_n(q) &= \sum_{k=0}^{n} q^{k(n-k)} = q^{n^2/4} \sum_{k=0}^{n} q^{-(k-n/2)^2}. \end{aligned}$$

Note that both $C(q)$ and $D(q)$ decrease to 1 as $q \to \infty$. If $q \ge 2$, then $C(q) \le C(2) < 9/4$ and $D(q) \le D(2) < 7/2$. The following estimates on Gaussian coefficients and Galois numbers were either obtained by Wilf [32] or follow from his work.

Lemma 4.2. *Fix $q \ge 2$. Then*

$$\begin{aligned} \begin{bmatrix} n \\ k \end{bmatrix}_q &\le D(q) q^{k(n-k)} \qquad (1) \\ D(q) q^{n^2/4 - 1/4} \left(2 - \frac{9q^{(1-n)/2}}{2}\right) &\le \mathcal{G}_n(q) \qquad (2) \\ &\le S_n(q) D(q) \\ &\le C(q) D(q) q^{n^2/4} \end{aligned}$$

Proof. Equation 1 and $\mathcal{G}_n(q) \le S_n(q)D(q)$ are proved in [32]. The inequality $S_n(q) \le C(q)q^{n^2/4}$ follows from Lemma 4.1, taking $f(x) = x(n-x) = -x^2 + nx$ and noting that $x(n-x) \le n^2/4$ for all x. This proves $\mathcal{G}_n(q) \le C(q)D(q)q^{n^2/4}$.

The lower bound for $\mathcal{G}_n(q)$ is slightly more complicated, but it is easy to see

from [32], Lemma 4.1, and the definition of $S_n(q)$ that

$$\begin{aligned}
\mathcal{G}_n(q) &\geq S_n(q) - \frac{2S_{n-1}(q) + 2q^{-2n}}{q-1} \\
&\geq 2q^{n^2/4-1/4} - \frac{2C(q)q^{(n-1)^2/4}}{q-1} \\
&\geq q^{n^2/4-1/4}\left(2 - \frac{2C(q)q^{(1-n)/2}}{q-1}\right) \\
&\geq q^{n^2/4-1/4}\left(2 - \frac{9q^{(1-n)/2}}{2}\right),
\end{aligned}$$

where the last inequality uses the fact that $2C(q)/(q-1) < 9/2$. □

Next we shall prove Lemma 4.3, which will be needed in Section 5 to bound products of Gaussian coefficients, and we will finish with Lemma 4.4, which will be used in Section 6.

Lemma 4.3. *Fix a prime p and integers $n \geq 3$ and $d \geq 6$ or $n \geq 10$ and $d \geq 5$. Let F be the free group on d generators, and let d_n be the rank of F_n/F_{n+1}. For $1 \leq i \leq n-1$ and $0 \leq u_i \leq d_i$, let*

$$A_i(u_i) = \sum \prod_{j=i}^{n-1} p^{-(u_{j+1}-d_{j+1})(u_{j+1}-u_j/2)},$$

where the sum is over all integers $u_{i+1}, \ldots, u_n$ such that

$$\begin{array}{lll}
0 \leq & u_j & \leq d_j \qquad \text{for } i+1 \leq j \leq n-2 \\
1 \leq & u_{n-1} & \leq d_{n-1} \\
2 \leq & u_n & \leq d_n.
\end{array}$$

Then for $1 \leq i \leq n-2$,

$$A_i(u_i) \leq C(p)^{n-i} p^{-15/16 + d_n^2/4 + d_{n-1} - d_n/4} p^{-u_i(d_{i+1}-1)/2}.$$

Proof. First note that

$$A_{n-1}(u_{n-1}) = \sum_{u_n=2}^{d_n} p^{-(u_n-d_n)(u_n-u_{n-1}/2)}.$$

As a function of u_n, the expression $-(u_n - d_n)(u_n - u_{n-1}/2)$ is at most $(d_n - u_{n-1}/2)^2/4$, so that

$$A_{n-1}(u_{n-1}) \leq C(p) p^{(d_n - u_{n-1}/2)^2/4}$$

by Lemma 4.1.

The proof of the theorem is by backward induction on i. Note that

$$A_i(u_i) = \sum_{u_{i+1}} p^{-(u_{i+1}-d_{i+1})(u_{i+1}-u_i/2)} A_{i+1}(u_{i+1}).$$

When $i = n-2$, using our bound on $A_{n-1}(u_{n-1})$ gives

$$\begin{aligned} & A_{n-2}(u_{n-2}) \\ \leq \; & C(p)p^{d_n^2/4} \sum_{u_{n-1}=1}^{d_{n-1}} p^{u_{n-1}^2/16 - u_{n-1}d_n/4 + (d_{n-1}-u_{n-1})(u_{n-1}-u_{n-2}/2)} \\ = \; & C(p)p^{d_n^2/4} \sum_{u_{n-1}=1}^{d_{n-1}} p^{-15u_{n-1}^2/16 + (-d_n/4 + u_{n-2}/2 + d_{n-1})u_{n-1} - d_{n-1}u_{n-2}/2} \end{aligned}$$

As a function of u_{n-1}, the polynomial

$$-15u_{n-1}^2/16 + (-d_n/4 + u_{n-2}/2 + d_{n-1})u_{n-1} - d_{n-1}u_{n-2}/2$$

is maximized at

$$u_{n-1} = 8(-d_n/4 + u_{n-2}/2 + d_{n-1})/15.$$

Computations show that this is at most 1 when $n \geq 3$ and $d \geq 6$ or $n \geq 10$ and $d \geq 5$. So as u_{n-1} ranges from 1 to d_{n-1}, the polynomial is maximized at $u_{n-1} = 1$. By Lemma 4.1 and the fact that $C(p^{15/16}) \leq C(p)$,

$$A_{n-2}(u_{n-2}) \quad \leq \quad C(p)^2 p^{d_n^2/4 - 15/16 - d_n/4 + d_{n-1}} p^{(1-d_{n-1})u_{n-2}/2}.$$

This proves the theorem for the base case $i = n-2$. By induction, for $i \leq n-3$,

$$\begin{aligned} A_i(u_i) \quad = \quad & \sum_{u_{i+1}=0}^{d_{i+1}} p^{-(u_{i+1}-d_{i+1})(u_{i+1}-u_i/2)} A_{i+1}(u_{i+1}) \\ \leq \quad & C(p)^{n-i-1} p^{-15/16 + d_n^2/4 + d_{n-1} - d_n/4} \\ & \cdot \sum_{u_{i+1}=0}^{d_{i+1}} p^{-(u_{i+1}-d_{i+1})(u_{i+1}-u_i/2) - u_{i+1}(d_{i+2}-1)/2}. \end{aligned}$$

As a function of u_{i+1}, the polynomial

$$\begin{aligned} & -(u_{i+1}-d_{i+1})(u_{i+1}-u_i/2) - u_{i+1}(d_{i+2}-1)/2) \\ = \quad & -u_{i+1}^2 + (d_{i+1} + u_i/2 - (d_{i+2}-1)/2)u_{i+1} - d_{i+1}u_i/i \end{aligned}$$

is maximized at

$$u_{i+1} = (d_{i+1} + u_i/i - (d_{i+2}-1)/2))/2.$$

Computations show that this is at most $1/2$ for $d \geq 3$ and $i \geq 1$. So as u_{i+1} ranges from 0 to d_{i+1}, the polynomial is maximized at $u_{i+1} = 0$. Thus

$$A_i(u_i) \leq C(p)^{n-i} p^{-15/16 + d_n^2/4 + d_{n-1} - d_n/4} p^{-(d_{i+1}-1)u_i/i}$$

and the result is proved by induction. □

Lemma 4.4. *Suppose that $\alpha_1, \ldots, \alpha_s$ are positive integers with $n = \alpha_1 + \cdots + \alpha_s$. Then*

$$\alpha_1^2 + \cdots + \alpha_s^2 \leq (n - s + 1)^2 + (s - 1), \tag{3}$$

and this bound is achieved when $\alpha_1 = \alpha_2 = \cdots = \alpha_{s-1} = 1$. Furthermore, if $n \geq \varepsilon + 1$ and $s \geq 2$, then

$$\alpha_1^2 + \cdots + \alpha_s^2 + \varepsilon s \leq (n - 1)^2 + 1 + 2\varepsilon. \tag{4}$$

Proof. For Equation 3, we use a simple induction argument. It is clearly true for $s = 1$. Suppose it is true up through s; we will prove it for $s + 1$.

$$\begin{aligned} \alpha_1^2 + \cdots + \alpha_s^2 + \alpha_{s+1}^2 &\leq (n - \alpha_{s+1} - s + 1)^2 + (s - 1) + \alpha_{s+1}^2 \\ &\leq (n - s + 1 - \alpha_{s+1})^2 + \alpha_{s+1}^2 + (s - 1) \\ &\leq (n - s + 1 - 1)^2 + 1^2 + (s - 1) \\ &= (n - s)^2 + s, \end{aligned}$$

proving Equation 3. As for Equation 4,

$$\begin{aligned} \alpha_1^2 + \cdots + \alpha_s^2 + \varepsilon s &\leq (n - s + 1)^2 + (s - 1) + \varepsilon s \\ &= ((n - 1) - (s - 2))^2 + s - 1 + \varepsilon s \\ &= (n - 1)^2 - 2(n - 1)(s - 2) + (s - 2)^2 + s - 1 + \varepsilon s \\ &\leq (n - 1)^2 - (\varepsilon + s - 1)(s - 2) + (s - 2)^2 + s - 1 + \varepsilon s \\ &= (n - 1)^2 + 1 + 2\varepsilon, \end{aligned}$$

where the first inequality follows from Equation 3 and the second inequality follows from the fact that since $n \geq \varepsilon + 1$ and $n \geq s$, we know that $n \geq (\varepsilon + s + 1)/2$. □

5 From Subgroups in F_2/F_{n+1} to Subgroups in F_n/F_{n+1}

The goal of this section is to prove Theorem 1.3, essentially showing that most $\mathrm{GL}(d, \mathbb{F}_p)$-orbits of normal subgroups of F/F_{n+1} contained in F_2/F_{n+1} are $\mathrm{GL}(d, \mathbb{F}_p)$-orbits of normal subgroups of F/F_{n+1} contained in F_n/F_{n+1}. We will prove Theorem 1.3 by estimating the number of normal subgroups of F/F_{n+1} contained in F_2/F_{n+1}. Theorem 5.1 offers a refined estimate on the number of normal subgroups of an arbitrary finite p-group. Our estimate depends on certain parameters which are difficult to work out in general, but have been calculated for F/F_{n+1} in Corollary 3.6. This will give us the tools to prove Theorem 1.3.

Let H be a finite p-group of lower p-length n. Given a normal subgroup U of H, note that by the second isomorphism theorem,

$$(U \cap H_i)/(U \cap H_{i+1}) \cong (U \cap H_i)H_{i+1}/H_{i+1},$$

and this quotient is elementary abelian. Let

$$S(H,\vec{u}) = \{U \lhd H \ : \ \dim((U \cap H_i)H_{i+1}/H_{i+1}) = u_i\},$$

where $\vec{u} = (u_1, \ldots, u_n)$ and each integer u_i satisfies

$$0 \leq u_i \leq h_i = \dim(H_i/H_{i+1}).$$

Theorem 5.1. *Suppose that for each $U \in S(H,\vec{u})$,*

$$\dim((U_2 \cap H_i)H_{i+1}/H_{i+1}) \geq v_i$$

and

$$\dim((U^p[U,H] \cap H_i)H_{i+1}/H_{i+1}) \geq w_i.$$

Then

$$|S(H,\vec{u})| \leq \begin{bmatrix} h_1 \\ u_1 \end{bmatrix}_p \prod_{i=2}^{n} \begin{bmatrix} h_i - w_i \\ u_i - w_i \end{bmatrix}_p p^{(u_1+\cdots+u_{i-1}-v_1-\cdots-v_{i-1})(h_i-u_i)}.$$

Proof. The proof proceeds by induction on n, the lower p-length of H. If $n = 1$, then H is elementary abelian of dimension h_1, so that $\vec{u} = (u_1)$ and $S(H,\vec{u}) = \begin{bmatrix} h_1 \\ u_1 \end{bmatrix}_p$.

Now suppose that the result holds in $J = H/H_n$, a group which has lower p-length $n-1$. Any normal subgroup U of H lying in $S(H,\vec{u})$ determines the subgroup $K = U \cap H_n$ of H_n and the normal subgroup $L = UH_n/H_n$ of J. The subgroup K contains $U^p[U,H] \cap H_n$, by hypothesis $\dim(U^p[U,H] \cap H_n) \geq w_n$, and $\dim(K) = \dim(U \cap H_n) = u_n$.

For $1 \leq i \leq n-1$, since $J_i = H_i/H_n$,

$$\begin{aligned} (L \cap J_i)J_{i+1}/J_{i+1} &= (UH_n/H_n \cap H_i/H_n)(H_{i+1}/H_n)/(H_{i+1}/H_n) \\ &\cong (UH_n \cap H_i)H_{i+1}/H_{i+1} \\ &\cong (U \cap H_i)H_{i+1}/H_{i+1}. \end{aligned} \tag{5}$$

Thus $L \in S(J,\vec{t}\,)$, where $\vec{t} = (u_1, \ldots, u_{n-1})$. Furthermore, if M is the inverse image of L in H, then

$$M^p[M,H] = (UH_n)^p[UH_n,H] = U^p[U,H],$$

since $H_{n+1} = H_n^p[H_n,H] = 1$. Thus L determines $U^p[U,H] \cap H_n$.

Given L, the subgroup K is a subspace of H_n of dimension u_n containing $M^p[M,H] \cap H_n$, which has dimension at least w_n. Let $w = \dim(M^p[M,H] \cap H_n)$. Then there are

$$\begin{bmatrix} h_n - w \\ u_n - w \end{bmatrix}_p = \begin{bmatrix} h_n - w \\ h_n - u_n \end{bmatrix}_p$$

choices for K. This Gaussian coefficient is a decreasing function of w, so there are at most

$$\begin{bmatrix} h_n - w_n \\ u_n - w_n \end{bmatrix}_p$$

choices for K. Hence the number of possible pairs K and L given by subgroups in $S(H, \vec{u})$ is at most

$$|S(J, \vec{t}\,)| \cdot \begin{bmatrix} h_n - w_n \\ u_n - w_n \end{bmatrix}_p .$$

There is a bijection between subgroups $U \in S(H, \vec{u})$ that give K and L and complements to H_n/K in M/K, given by $U \mapsto U/K$. In the one direction, U/K is a complement to H_n/K since $U \cap H_n = K$ and $UH_n/K = M/K$. In the other direction, a complement U/K to H_n/K satisfies $U \cap H_n = K$ and $UH_n/K = M/K$, so U gives K and L.

Recall that in general, if G is a group with normal subgroup N, then the number of complements to N in G is either 0 or $|\mathrm{Der}(G/N, N)|$. When N is central, $\mathrm{Der}(G/N, N) = \mathrm{Hom}(G/N, N)$, and if the number of complements is 0, then $\mathrm{Hom}(G/N, N)$ is trivial (see Lubotzky and Segal [18, Lemma 1.3.1]).

Since H_n/K is central in M/K ($H_n \in Z(H)$), the number of complements to H_n/K in M/K is

$$|\mathrm{Hom}(M/H_n, H_n/K)| = |\mathrm{Hom}(L, H_n/K)| = |\mathrm{Hom}(L/L_2, H_n/K)|.$$

The dimension of $H_n/K = H_n/(H_n \cap U)$ is $h_n - u_n$. Also,

$$\begin{aligned} & \dim(L/L_2) \\ = \; & \dim(L) - \dim(L_2) \\ = \; & \sum_{i=1}^{n-1} \dim((L \cap J_i)J_{i+1}/J_{i+1}) - \sum_{i=1}^{n-1} \dim((L_2 \cap J_i)J_{i+1}/J_{i+1}). \end{aligned}$$

Note that $L_2 = U_2 H_n/H_n$, and a similar calculation to Equation 5 shows that

$$(L_2 \cap J_i)J_{i+1}/J_{i+1} \cong (L_2 \cap H_i)H_{i+1}/H_{i+1},$$

which by hypothesis has dimension at least v_i. Thus

$$\dim(L/L_2) \leq u_1 + \cdots + u_{n-1} - (v_1 + \cdots + v_{n-1})$$

and

$$|\mathrm{Hom}(L/L_2, H_n/K)| \leq p^{(h_n - u_n)(u_1 + \cdots + u_{n-1} - v_1 - \cdots - v_{n-1})}.$$

Using the inductive hypothesis gives

$$\begin{aligned} S(H, \vec{u}) &\leq S(J, \vec{t}\,) \cdot \begin{bmatrix} h_n - u_n \\ u_n - w_n \end{bmatrix}_p \cdot p^{(h_n - u_n)(u_1 + \cdots + u_{n-1} - v_1 - \cdots - v_{n-1})} \\ &\leq \begin{bmatrix} h_1 \\ u_1 \end{bmatrix}_p \prod_{i=2}^{n} \begin{bmatrix} h_i - w_i \\ u_i - w_i \end{bmatrix}_p p^{(u_1 + \cdots + u_{i-1} - v_1 - \cdots - v_{i-1})(H_i - u_i)}. \end{aligned}$$

□

We can now prove Theorem 1.3, restated here for convenience.

Theorem 1.3. *Fix a prime p and integers d and n so that either $n \geq 3$ and $d \geq 6$ or $n \geq 10$ and $d \geq 5$. Let F be the free group on d generators and let d_n be the rank of F_n/F_{n+1}. Then*

$$1 \leq \frac{|\mathfrak{A}_{d,n}|}{|\mathfrak{C}_{d,n}|} \leq 1 + C(p)^{n-1} D(p)^{n-2} p^{d_{n-1} - d_n/4 + d^2}.$$

Proof. To prove this result, we need to apply the estimates of Lemmas 4.2 and 4.3 to the upper bound for $S(H, \vec{u})$ obtained in Theorem 5.1 in the case when $H = F/F_{n+1}$. By Corollary 3.6, we may choose $v_{i+1} = u_i$ and $w_{i+1} = (3/2)u_i$. In particular, $w_{i+1} = 0$ if $u_i = 0$. By Equation 1 of Lemma 4.2, we have

$$\begin{bmatrix} n \\ k \end{bmatrix}_p \leq D(p) p^{k(n-k)}.$$

Substituting in the bound obtained in Theorem 5.1, we find that, if $u_1 = 0$, then

$$|S(H, \vec{u})| \leq D(p)^{n-1} p^h,$$

where

$$\begin{aligned} h &= u_2(d_2 - u_2) + (u_3 - w_3)(d_3 - u_3) + \cdots + (u_n - w_n)(d_n - u_n) \\ &\qquad + u_2(d_3 - u_3) + \cdots + u_{n-1}(d_n - u_n) \\ &\leq -(u_2 - d_2)u_2 - (u_3 - d_3)(u_3 - u_2/2) - \cdots \\ &\qquad - (u_n - d_n)(u_n - u_{n-1}/2). \end{aligned}$$

Hence

$$|\mathcal{A}_{d,n}| \leq |\mathcal{C}_{d,n}| + \sum_{\vec{u}} D(p)^{n-1} p^h = |\mathcal{C}_{d,n}| + D(p)^{n-1} \sum_{\vec{u}} p^h,$$

where the sum is taken over all $\vec{u}$ such that $U \in S(H, \vec{u})$ if and only if $U \leq F_2/F_{n+1}$ and $U \not\leq F_n/F_{n+1}$. In terms of $\vec{u}$, this means that $u_{n-1} \geq 1$ and $u_1 = 0$. Since $u_n \geq w_n > u_{n-1}$, we know that $u_n \geq 2$. Then by Lemma 4.3, we have

$$\sum_{\vec{u}} p^h = A_1(0),$$

and

$$|\mathcal{A}_{d,n}| \leq |\mathcal{C}_{d,n}| + D(p)^{n-1} C(p)^{n-1} p^y,$$

where

$$y = d_n^2/4 - 15/16 - d_n/4 + d_{n-1}.$$

Hence, as $|\mathcal{C}_{d,n}| = \mathcal{G}_{d_n}(p)$, using Lemma 4.2 and the fact that $2 - 9p^{(1-d_n)/2}/2 > 1$,

$$\begin{aligned} |\mathcal{A}_{d,n}|/|\mathcal{C}_{d,n}| &\leq 1 + D(p)^{n-1} C(p)^{n-1} p^y / \mathcal{G}_{d_n}(p) \\ &\leq 1 + D(p)^{n-2} C(p)^{n-1} p^{d_{n-1} - d_n/4}. \end{aligned}$$

Now by Theorems 2.7 and 2.8, $|\mathfrak{A}_{d,n}|$ and $|\mathfrak{C}_{d,n}|$ are the number of $\mathrm{GL}(d,\mathbb{F}_p)$-orbits on $\mathcal{A}_{d,n}$ and $\mathcal{C}_{d,n}$ respectively. Hence

$$0 \leq |\mathfrak{A}_{d,n}| - |\mathfrak{C}_{d,n}| \leq |\mathcal{A}_{d,n}| - |\mathcal{C}_{d,n}|,$$

since $|\mathfrak{A}_{d,n}| - |\mathfrak{C}_{d,n}|$ is the number of $\mathrm{GL}(d,\mathbb{F}_p)$ orbits in $\mathcal{A}_{d,n} \setminus \mathcal{C}_{d,n}$. Also $|\mathcal{C}_{d,n}| \leq |\mathfrak{C}_{d,n}| \cdot |\mathrm{GL}(d,\mathbb{F}_p)|$, since $\mathcal{C}_{d,n}$ falls into $|\mathfrak{C}_{d,n}|$ orbits, each of size at most $|\mathrm{GL}(d,\mathbb{F}_p)|$. Then

$$\begin{aligned} 0 &\leq \frac{|\mathfrak{A}_{d,n}|}{|\mathfrak{C}_{d,n}|} - 1 \\ &= \frac{|\mathcal{C}_{d,n}|}{|\mathfrak{C}_{d,n}|}\left(\frac{|\mathfrak{A}_{d,n}| - |\mathfrak{C}_{d,n}|}{|\mathcal{C}_{d,n}|}\right) \\ &\leq |\mathrm{GL}(d,\mathbb{F}_p)|\left(\frac{|\mathcal{A}_{d,n}| - |\mathcal{C}_{d,n}|}{|\mathcal{C}_{d,n}|}\right) \\ &\leq C(p)^{n-1}D(p)^{n-2}p^{d_{n-1}-d_n/4+d^2}. \end{aligned}$$

Therefore

$$1 \leq \frac{|\mathfrak{A}_{d,n}|}{|\mathfrak{C}_{d,n}|} \leq 1 + C(p)^{n-1}D(p)^{n-2}p^{d_{n-1}-d_n/4+d^2}.$$

□

6 Most Orbits on Subgroups of F_n/F_{n+1} are Regular

In this section we shall prove Theorem 1.4. This depends on estimating $|\mathfrak{C}_{d,n}|$, the number of $\mathrm{GL}(d,\mathbb{F}_p)$-orbits on subspaces of F_n/F_{n+1}, via the Cauchy-Frobenius Lemma. To do this, we obtain in Theorem 6.2 an upper bound for the number of subspaces of F_n/F_{n+1} fixed by an element of $\mathrm{GL}(d,\mathbb{F}_p)$, and refine this in Theorem 6.3 to obtain a stronger bound in the case $n = 2$.

Suppose M is an $\mathbb{F}_p\mathrm{GL}(d,\mathbb{F}_p)$-module. Let $g \in \mathrm{GL}(d,\mathbb{F}_p)$. We want to count the number of subspaces of M (viewed as an $\mathbb{F}_p$-vector space) fixed by g, which is the number of submodules of M as a $\mathbb{F}_p\langle g\rangle$-module. We note that when M is the natural $\mathbb{F}_p\mathrm{GL}(d,\mathbb{F}_p)$-module, Eick and O'Brien [5] give an explicit formula for this number. The following preliminaries are based on Macdonald [19, Chapter IV, Section 2].

Let Φ be the set of all polynomials in $\mathbb{F}_p[t]$ which are irreducible over $\mathbb{F}_p$ and let P be the set of all partitions of non-negative integers. Let U be the set of all functions $\mu : \Phi \to P$ such that $m = \sum_{f\in\Phi} \deg(f)|\mu(f)|$, where $|\mu(f)|$ is the sum of the parts of the partition $\mu(f)$. Then there is a one-to-one correspondence between $\mathbb{F}_p\langle g\rangle$-modules M of dimension m and functions $\mu \in U$. This correspondence is given by

$$M \cong \bigoplus_{f\in\Phi}\bigoplus_i \frac{\mathbb{F}_p[t]}{(f)^{\mu_i(f)}},$$

where $\mu_i(f)$ is the i-th part of $\mu(f)$, (f) is the ideal of $\mathbb{F}_p[t]$ generated by f, and g acts upon $\mathbb{F}_p[t]/(f)^s$ as multiplication by t.

Let

$$M_f = \bigoplus_i \frac{\mathbb{F}_p[t]}{(f)^{\mu_i(f)}}.$$

We call $\mu(f)$ the *type* of M_f. Any submodule N of M can be written $N = \oplus_{f\in\Phi} N_f$ with $N_f \subseteq M_f$ for each $f \in \Phi$. That is, every submodule of M is the direct sum of submodules of the summands M_f. By Macdonald [19, Chapter II, 3.1] the type λ of any $\mathbb{F}_p\langle g\rangle$-submodule or quotient module of M_f satisfies $\lambda \subseteq \mu(f)$.

For each $f \in \Phi$, let $\mathbb{F}_p[t]_f$ denote the localization of $\mathbb{F}_p[t]$ at the prime ideal (f). Then $\mathbb{F}_p[t]_f$ is a discrete valuation ring with residue field of order $q = p^{\deg(f)}$ and M_f is a finite $\mathbb{F}_p[t]_f$-module of type $\mu(f)$.

Both Theorems 6.2 and 6.3 depend on Theorem 6.1, where we calculate the number of submodules of fixed type in a module of fixed type over a discrete valuation ring. This generalizes the formula for the number of subgroups of a finite abelian p-group (see Birkhoff [2]).

Theorem 6.1. *Let $\mathfrak{a}$ be a discrete valuation ring with maximal ideal $\mathfrak{p}$ and let $\mathfrak{k} = \mathfrak{a}/\mathfrak{p}$ be the residue field of order q. Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_s)$ and $\beta = (\beta_1, \beta_2, \ldots, \beta_r)$ be partitions with $\beta \subseteq \alpha$ and let M be a finite $\mathfrak{a}$-module of type α'. Then the number of submodules of M of type β' is*

$$S(\alpha', \beta', q) = \prod_{i=1}^{r} \begin{bmatrix} \alpha_i - \beta_{i+1} \\ \beta_i - \beta_{i+1} \end{bmatrix}_q q^{\beta_{i+1}(\alpha_i - \beta_i)}.$$

Proof. The proof is by induction on β_1. If $\beta_1 = 0$, then $S(\alpha', \beta', q) = 1$ and the result holds. Suppose $\beta_1 > 0$, and let the smallest part of β' be t, so that either $\beta_1 = \cdots = \beta_t > \beta_{t+1}$ and $t < s$, or $\beta_1 = \cdots = \beta_s$ and $t = s$. Write

$$\overline{\beta} = (\beta_1 - 1, \beta_2 - 1, \ldots, \beta_t - 1, \beta_{t+1}, \ldots).$$

Let N be any submodule of M of type $\overline{\beta}'$, and le tx be any element of M with $\mathfrak{p}^t x = 0$, $\mathfrak{p}^{t-1} x \neq 0$, and $\mathfrak{p}x \cap N = 0$. Then $\langle N, x\rangle$ has type β'. There are $S(\alpha', \overline{\beta}', q)$ choices for N, and for each N it follows from [19, Chapter II, Equation 1.8] that the number of choices for x is just

$$q^{\alpha_1 + \cdots + \alpha_t}(1 - q^{\beta_t - \alpha_t - 1}). \tag{6}$$

On the other hand, fix a submodule L of M of type β'; we can count the number of choices of N and x so that $L = \langle N, x\rangle$. Here N is a submodule of L of type $\overline{\beta}'$ whose quotient has type (t), and by [19, Chapter II, Equation 4.13], the number of choices for N is

$$\frac{1 - q^{\beta_{t+1} - \beta_t}}{1 - q^{-1}} q^{\sum_i \binom{\beta_i}{2} - \sum_i \binom{\overline{\beta}_i}{2}} = \frac{1 - q^{\beta_{t+1} - \beta_t}}{1 - q^{-1}} q^{t(\beta_t - 1)}.$$

Given N, it follows from [19, Chapter II, Equation 1.8] that there are

$$q^{\beta_1+\cdots+\beta_t}(1-q^{-1})$$

choices for x. Thus any submodule L of M of type β' arises as $\langle N, x\rangle$ in

$$q^{\beta_1+\cdots+\beta_t+t(\beta_t-1)}(1-q^{\beta_{t+1}-\beta_t})$$

ways. The total number of submodules L of M of type β' is then

$$\begin{aligned} S(\alpha',\beta',q) &= \frac{S(\alpha',\overline{\beta}',q)q^{\alpha_1+\cdots+\alpha_t}(1-q^{\beta_t-\alpha_t-1})}{q^{\beta_1+\cdots+\beta_t+t(\beta_t-1)}(1-q^{\beta_{t+1}-\beta_t})} \\ &= \frac{S(\alpha',\overline{\beta}',q)q^{\alpha_1+\cdots+\alpha_t}(1-q^{\beta_t-\alpha_t-1})}{q^{2t\beta_t-t}(1-q^{\beta_{t+1}-\beta_t})}, \end{aligned} \tag{7}$$

where the second inequality uses $\beta_1=\cdots=\beta_t$. By induction, we know that

$$\begin{aligned} S(\alpha',\overline{\beta}',q) &= \prod_{i=1}^{r}\begin{bmatrix}\alpha_i-\overline{\beta}_{i+1}\\ \overline{\beta}_i-\overline{\beta}_{i+1}\end{bmatrix}_q q^{\overline{\beta}_{i+1}(\alpha_i-\overline{\beta}_i)} \\ &= \prod_{i=1}^{t-1}\begin{bmatrix}\alpha_i-\beta_{i+1}+1\\ \beta_i-\beta_{i+1}\end{bmatrix}_q q^{(\beta_{i+1}-1)(\alpha_i-\beta_i+1)} \\ &\qquad \cdot\begin{bmatrix}\alpha_t-\beta_{t+1}\\ \beta_t-\beta_{t+1}-1\end{bmatrix}_q q^{\beta_{t+1}(\alpha_t-\beta_t+1)} \\ &\qquad \cdot\prod_{i=t+1}^{r}\begin{bmatrix}\alpha_i-\beta_{i+1}\\ \beta_i-\beta_{i+1}\end{bmatrix}_q q^{\beta_{i+1}(\alpha_i-\beta_i)} \\ &= \prod_{i=1}^{r}\begin{bmatrix}\alpha_i-\beta_{i+1}\\ \beta_i-\beta_{i+1}\end{bmatrix}_q q^{\beta_{i+1}(\alpha_i-\beta_i)} \\ &\qquad \cdot\prod_{i=1}^{t-1}\frac{q^{\alpha_i-\beta_{i+1}+1}-1}{q^{\alpha_i-\beta_i+1}-1}q^{\beta_{i+1}+\beta_i-\alpha_i-1}\cdot\frac{q^{\beta_t-\beta_{t+1}}-1}{q^{\alpha_t-\beta_t+1}-1}q^{\beta_{t+1}} \\ &= \prod_{i=1}^{r}\begin{bmatrix}\alpha_i-\beta_{i+1}\\ \beta_i-\beta_{i+1}\end{bmatrix}_q q^{\beta_{i+1}(\alpha_i-\beta_i)} \\ &\qquad \cdot q^{2(t-1)\beta_t-\alpha_1-\cdots-\alpha_{t-1}-(t-1)}\cdot\frac{q^{\beta_t-\beta_{t+1}}-1}{q^{\alpha_t-\beta_t+1}-1}q^{\beta_{t+1}} \\ &= \prod_{i=1}^{r}\begin{bmatrix}\alpha_i-\beta_{i+1}\\ \beta_i-\beta_{i+1}\end{bmatrix}_q q^{\beta_{i+1}(\alpha_i-\beta_i)}\cdot\frac{q^{2t\beta_t}}{q^{\alpha_1+\cdots+\alpha_t+t}}\cdot\frac{1-q^{\beta_{t+1}-\beta_t}}{1-q^{\beta_t-\alpha_t-1}}. \end{aligned}$$

Substituting this expression into Equation 7 gives the result. □

Using Theorem 6.1 and the techniques of Section 4, we can give an upper bound for the total number of submodules of a finite $\mathbb{F}_p\langle g\rangle$-module M. Note that every subspace of M is a $\mathbb{F}_p\langle g\rangle$-module if and only if g acts as a scalar on M, that is, as multiplication by an element of $\mathbb{F}_p$.

Theorem 6.2. *Fix $d \geq 2$ and $g \in \mathrm{GL}(d, \mathbb{F}_p)$. Suppose that M is an $\mathbb{F}_p\langle g \rangle$-module. Let $m = \dim_{\mathbb{F}_p}(M)$ and let S_M be the number of submodules of M. Then either g acts as a scalar on M and $S_M = \mathcal{G}_m(p)$, or g does not act as a scalar and*

$$\log_p S_M \leq (m^2 - 2m + 2)/4 + 2\varepsilon,$$

where $\varepsilon = \log_p(C(p)D(p))$.

Proof. Write $M = \oplus_{i=1}^{k} M_i$, where for each i, $M_i = M_{f_i}$ for some $f_i \in \Phi$ and $\dim_{\mathbb{F}_p} M_i = m_i$.

Case 1: $k \geq 2$.

Each submodule of M is a direct sum of submodules of the summands M_i, so $S_M = \prod_{i=1}^{k} S_{M_i} \leq \mathcal{G}_{m_1}(p)\mathcal{G}_{m-m_1}(p)$. Then by Lemma 4.2,

$$S_M \leq C(p)^2 D(p)^2 p^{m_1^2/4 + (m-m_1)^2/4} \leq C(p)^2 D(p)^2 p^{(m^2-2m+2)/4},$$

since $0 < m_1 < m$.

Case 2: $k = 1$.

In this case, $M = M_f$ for some $f \in \Phi$. Let $u = \deg(f)$ and $q = p^u$, and let M have type α' as a $\mathbb{F}_p[t]_f$-module, where $\alpha = (\alpha_1, \ldots, \alpha_s)$.

Subcase 2.1: α has at least two parts.

If $\beta = (\beta_1, \ldots, \beta_r)$ and $\beta \subseteq \alpha$, then by Theorem 6.1 and Lemma 4.2 Equation 1, the number of submodules of M of type β' is

$$\begin{aligned} S(\alpha', \beta', q) &\leq \prod_{i=1}^{r} D(q) q^{(\beta_i - \beta_{i+1})(\alpha_i - \beta_i) + \beta_{i+1}(\alpha_i - \beta_i)} \\ &= D(q)^r \prod_{i=1}^{r} q^{\beta_i(\alpha_i - \beta_i)}. \end{aligned}$$

Thus

$$\begin{aligned} S_M &= \sum_{\beta' \subseteq \alpha'} S(\alpha', \beta', q) \\ &\leq D(q)^s \sum_{\beta' \subseteq \alpha'} \prod_{i=1}^{r} q^{\beta_i(\alpha_i - \beta_i)} \\ &\leq D(q)^s \prod_{i=1}^{s} \sum_{b_i=0}^{\alpha_i} q^{b_i(\alpha_i - b_i)} \\ &\leq D(q)^s C(q)^s \prod_{i=1}^{s} q^{\alpha_i^2/4}, \end{aligned}$$

where the last inequality follows from Lemma 4.1. Now $D(q) \leq D(p)$ and $C(q) \leq C(p)$ so, remembering that $u(\alpha_1 + \cdots + \alpha_s) = m$ and using Lemma 4.4,

$$\begin{aligned} \log_p S_M &\leq u(\alpha_1^2 + \cdots + \alpha_s^2)/4 + s\varepsilon \qquad (8) \\ &\leq (4s\varepsilon + (u\alpha_1)^2 + \cdots + (u\alpha_s)^2 + 4s\varepsilon)/4 \\ &\leq ((m-1)^2 + 1 + 8\varepsilon)/4 \\ &\leq (m^2 - 2m + 2)/4 + 2\varepsilon, \end{aligned}$$

if $m \geq 4\varepsilon + 1$. For $m < 4\varepsilon + 1$,

$$\begin{aligned} \log_p S_M &\leq m^2/4 \\ &\leq (m^2 - 2m + 2)/4 + (m-1)/2 \\ &\leq (m^2 - 2m + 2)/4 + 2\varepsilon. \end{aligned}$$

Subcase 2.2: α has one part.

In this case, $\alpha_1 = m/u$. If $u \geq 2$, then by Lemma 4.2 Equation 1,

$$\begin{aligned} S_M &= \sum_{0 \leq \beta_1 \leq \alpha_1} \begin{bmatrix} \alpha_1 \\ \beta_1 \end{bmatrix}_q \\ &\leq C(q)D(q)q^{m^2/4u^2} \\ &\leq C(p)^2 D(p)^2 p^{m^2/4u} \\ &\leq C(p)^2 D(p)^2 p^{(m^2-2m+2)/4}, \end{aligned}$$

since $u \geq 2$. On the other hand, if $u = 1$, then $f = t - c$ for some $c \in \mathbb{F}_p$ and $M \cong \oplus^m \{\mathbb{F}_p[t]/(f)\}$ so that g acts as the scalar c on M and $S_M = \mathcal{G}_m(p)$. □

The next theorem strengthens this result when the module structure is known more precisely and will be needed to deal with groups of lower p-length 2.

Theorem 6.3. *Fix $d \geq 2$ and $g \in \mathrm{GL}(d, \mathbb{F}_p)$ with $g \neq 1$. Suppose that V is an $\mathbb{F}_p\langle g \rangle$-module on which g acts non-trivially and that M is an $\mathbb{F}_p\langle g \rangle$-module extension of $V \wedge V$ by V. Let $v = \dim_{\mathbb{F}_p}(V)$, let $m = \dim_{\mathbb{F}_p}(M) = v(v+1)/2$, and let S_M be the number of submodules of M. Then*

$$\log_p S_M \leq (m-4)^2/4 + C,$$

where $\varepsilon = \log_p(C(p)D(p))$ and

$$C = \begin{cases} \varepsilon + 2m - 4 & : \quad m \leq 45 \\ 5\varepsilon + 4 & : \quad \textit{otherwise.} \end{cases}$$

Proof. First, if $v \leq 9$, then $m \leq 45$. In this case,

$$\begin{aligned} S_M &\leq \mathcal{G}_m(p) \\ &\leq C(p)D(p)p^{m^2/4} \\ &= C(p)D(p)p^{(m-4)^2/4+2m-4}, \end{aligned}$$

proving the result. So we may assume that $v \geq 10$.

Write $M = \oplus_{i=1}^{k} M_i$, where for each i, $M_i = M_{f_i}$ for some $f_i \in \Phi$ and $\dim_{\mathbb{F}_p} M_i = m_i$; we may assume that $m_1 \geq m_2 \geq \cdots \geq m_k$. Note that $m_1 + \cdots + m_k = m$. Then $V = \oplus_{i=1}^{m} M_i\pi$ where π is the projection from M onto V.

Fix $0 < t < k$ and set $W = M_1 \oplus \cdots \oplus M_t$. Also let $w = \dim W = m_1 + \cdots + m_t$. Then $S_M \leq \mathcal{G}_w(p)\mathcal{G}_{M-w}(p)$ since any submodule of M is a direct sum of submodules of the summands M_i. By Lemma 4.2,

$$S_M \leq C(p)^2 D(p)^2 p^{w^2/4 + (M-w)^2/4}.$$

When $4 \leq w \leq M-4$, it follows that

$$\begin{aligned} S_M &\leq C(p)^2 D(p)^2 p^{4 + (M-4)^2/4} \text{ and} \\ \log_p S_M &\leq (M-4)^2/4 + 2\varepsilon + 4, \end{aligned}$$

proving the result. If we cannot choose t so that $4 \leq w \leq m-4$, then since $m > 9$ implies that $m_1 \not\leq 3$, it must be that $m_1 \geq m-3$ and $k \leq 4$. Write $Y = M_2 \oplus \cdots \oplus M_k$; then $y = \dim Y \leq 3$. (It is possible that Y is the zero module and that $y = 0$.) At this point we need to prove a technical claim which we will use twice.

Claim: Suppose that V is the direct sum of $\mathbb{F}_p\langle g \rangle$-modules A and B of dimensions $a \geq 4$ and $v - a$ over $\mathbb{F}_p$, and suppose that $A \subset M_1\pi$. If g acts as a scalar c on A, then $c = 1$ and $A \otimes B$ is the direct sum of a copies of B.

Proof of claim: If $V = A \oplus B$, then $V \wedge V \cong (A \wedge A) \oplus (B \wedge B) \oplus (A \otimes B)$. If g acts as a scalar c on A, then $A \cong \oplus\{\mathbb{F}_p[t]/(t-c)\}^a$ and $M_1 = M_{f_1}$ with $f_1 = t - c$. In this case g acts as the scalar c^2 on $A \wedge A$, so $A \wedge A \cong \{\mathbb{F}_p[t]/(t-c^2)\}^{a(a-1)/2}$. If $c \neq 1$, then $A \wedge A \not\subseteq M_1$ and hence $A \wedge A \subseteq Y$. But then $a(a-1)/2 = \dim(A \wedge A) \leq \dim Y \leq 3$, which is impossible. Therefore $c = 1$. Since g acts on V non-trivially, the action on B is non-trivial and $A \otimes B$ is the direct sum of a copies of B.

Now take $A = M_1\pi$ and $B = Y\pi$ so that $V = A \oplus B$. Suppose that g acts on A as a scalar c. Since $v \geq 7$ and $\dim B \leq \dim Y \leq 3$, we see that $a \geq 4$, and by the claim, $c = 1$ and $A \otimes B$ is the direct sum of a copies of B. If B is the zero module, this contradicts the fact that g acts non-trivially on V. Otherwise, $v - a > 0$. Since B is the image of Y, it follows that $A \otimes B \subseteq Y$, and $a(v-a) \leq \dim Y \leq 3$, which is false. Therefore g does not act on $M_1\pi$ as a scalar, and hence does not act on M_1 as a scalar.

We may assume that $M_1 = M_f$ where f has degree u over $\mathbb{F}_p$ and M_1 and $M_1\pi$ have types α' and β' respectively, where $\beta \subseteq \alpha$. Write $\alpha = (\alpha_1, \ldots, \alpha_s)$ and $\beta = (\beta_1, \ldots, \beta_r)$.

Case 1: $u > 1$.

Writing S_{M_1} for the number of submodules of M_1, we have

$$\begin{aligned} S_{M_1} &\leq \mathcal{G}_{m_1/u}(q) \\ &\leq C(q)D(q)q^{m_1^2/4u^2} \\ &\leq C(p)D(p)p^{m_1^2/4u} \\ &\leq C(p)D(p)p^{m_1^2/8}. \end{aligned}$$

Then

$$\begin{aligned} S_M &\leq S_{M_1}\mathcal{G}_y(p) \\ &\leq C(p)^2D(p)^2p^{m_1^2/8+y^2/4} \\ &\leq C(p)^2D(p)^2p^{m^2/8+9/4} \\ &\leq C(p)^2D(p)^2p^{(m-4)^2/4+9/4}, \end{aligned}$$

where the last line uses the fact that $m \geq 14$. Thus $\log_p S_M \leq C + (m-4)^2/4$.

Case 2: $u = 1$.

In this case, $f = t - c$ for some $c \in \mathbb{F}_p$. Since g does not act as a scalar on M_1 or $M_1\pi$, $\alpha_2 \geq \beta_2 > 0$.

By Equation 8,

$$\log_p S_M \leq (\alpha_1^2 + \cdots + \alpha_s^2)/4 + s\varepsilon,$$

so

$$\log_p S_M \leq \log_p S_{M_1} + \log_p \mathcal{G}_y(p) \leq (\alpha_1^2 + \cdots + \alpha_s^2 + y^2)/4 + (s+1)\varepsilon.$$

Subcase 2.1: $\alpha_1 \leq m - 4$

If $s = 2$, then

$$\begin{aligned} \log_p S_M &\leq (\alpha_1^2 + \alpha_2^2 + y^2)/4 + 3\varepsilon \\ &\leq ((m-4)^2 + 4^2 + 0^2)/4 + 3\varepsilon \\ &\leq (m-4)^2/4 + C. \end{aligned}$$

If $s = 3$, then

$$\begin{aligned} \log_p S_M &\leq (\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + y^2)/4 + 4\varepsilon \\ &\leq ((m-4)^2 + 3^2 + 1^2 + 0^2)/4 + 4\varepsilon \\ &\leq (m-4)^2/4 + C. \end{aligned}$$

Finally, if $4 \leq s \leq m$, then by Lemma 4.4, we get

$$\log_p S_M \leq ((m-s)^2 + s)/4 + (s+1)\varepsilon.$$

The right-hand side is maximized at $s = 4$ or $s = m$. Since $m > 45$ and $\varepsilon \leq 6$, it turns out that it is maximized at $s = 4$, where we get a bound of $(m-4)^2/4 + 5\varepsilon + 1$.

Subcase 2.2: $\alpha_1 \geq m - 3$.

So we may assume that $\alpha_1 \geq m - 3$. Then $\alpha_2 + \cdots + \alpha_s + y \leq 3$, and so $\beta_2 + \cdots + \beta_r + \dim(\pi Y) \leq 3$. Since $\beta_1 + \cdots + \beta_r + \dim(\pi Y) = v \geq 10$, it follows that $\beta_1 \geq 7$ and $\beta_1 - \beta_2 \geq 4$. Note that $\beta_1 - \beta_2$ is the number of summands of $M_1\pi$ that are isomorphic to $\mathbb{F}_p[t]/(f-c)$. So write $M_1\pi = A \oplus C$, where $a = \dim A = \beta_1 - \beta_2$ and g acts as the scalar c on A and not on C. Set $B = C \oplus Y\pi$. Then $V = A \oplus B$ and by the claim, $c = 1$ and $A \otimes B$ is a direct sum of a copies of B. Then $A \otimes B$ is contained in Y plus the components of M_1 that g does not act as a scalar on, so that $a\beta_2 \leq \dim(A \otimes B) \leq \alpha_2 + y \leq 3$, which is impossible. □

We can now prove Theorem 1.4, restated here for convenience.

Theorem 1.4. *Fix a prime p and integers d and n so that either $n = 2$ and $d \geq 10$ or $n \geq 3$ and $d \geq 3$. Let F be the free group on d generators and let d_n be the rank of F_n/F_{n+1}. Let*

$$K = \begin{cases} C(p)^5 D(p)^4 p^{17/4} & : \quad n = 2 \text{ and } d \geq 10 \\ C(p)^2 D(p) p^{3/4} & : \quad n \geq 3. \end{cases}$$

Let

$$x = \begin{cases} -d & : \quad n = 2 \\ d^2 - d_n/2 & : \quad n \geq 3. \end{cases}$$

Then

(a)
$$1 \leq \frac{|\mathfrak{C}_{d,n}| \cdot |\mathrm{GL}(d, \mathbb{F}_p)|}{|\mathcal{C}_{d,n}|} \leq 1 + Kp^x.$$

(b)
$$1 \leq \frac{|\mathfrak{C}_{d,n}|}{|\mathfrak{D}_{d,n}|} \leq \frac{1 + Kp^x}{1 - Kp^x}.$$

Proof. Recall that $\mathfrak{C}_{d,n}$ is the set of $\mathrm{GL}(d, \mathbb{F}_p)$-orbits in $\mathcal{C}_{d,n}$, $\mathfrak{D}_{d,n}$ is the set of regular orbits in $\mathfrak{C}_{d,n}$ (that is, the orbits in which every point has trivial stabilizer), and $|\mathcal{C}_{d,n}| = \mathcal{G}_{d_n}(p)$. If $g \in \mathrm{GL}(d, \mathbb{F}_p)$, then $|(\mathcal{C}_{d,n})^g|$, the number of elements of $\mathcal{C}_{d,n}$ fixed by g, is just the number of submodules of F_n/F_{n+1} viewed as a $\mathbb{F}_p\langle g \rangle$-module, which we estimated in Theorems 6.2 and 6.3.

We explain first why only the identity element of $\mathrm{GL}(d, \mathbb{F}_p)$ can act as a scalar on F_n/F_{n+1}. By Theorem 3.2, F_n/F_{n+1} has a $\mathbb{F}_p\mathrm{GL}(d, \mathbb{F}_p)$-submodule M which is isomorphic to an extension of $V \wedge V$ by V, where V is the natural $\mathbb{F}_p\mathrm{GL}(d, \mathbb{F}_p)$-module. If $g \in \mathrm{GL}(d, \mathbb{F}_p)$ acts on F_n/F_{n+1} as a scalar $c \in \mathbb{F}_p$, then

it acts on V as the scalar c, and hence on $V \wedge V$ as the scalar c^2. Thus $c = c^2$ and $c = 1$, so that g is the identity on V, that is, the identity element in $\mathrm{GL}(d, \mathbb{F}_p)$.

Suppose first that $n > 2$. We know from Theorem 6.2 that if $g \neq 1$,

$$|(\mathcal{C}_{d,n})^g| \leq C(p)^2 D(p)^2 p^{(d_n^2 - 2d_n + 2)/4}.$$

By the Cauchy-Frobenius Lemma,

$$\begin{aligned} |\mathrm{GL}(d, \mathbb{F}_p)| \cdot |\mathfrak{C}_{d,n}| &= \sum_{g \in \mathrm{GL}(d, \mathbb{F}_p)} |(\mathcal{C}_{d,n})^g| \\ &= |\mathcal{C}_{d,n}| + \sum_{g \neq 1} |(\mathcal{C}_{d,n})^g| \\ &\leq |\mathcal{C}_{d,n}| + (|\mathrm{GL}(d, \mathbb{F}_p)| - 1) C(p)^2 D(p)^2 p^{(d_n^2 - 2d_n + 2)/4}. \end{aligned}$$

By Lemma 4.2 Equation 2 and the fact that $2 - 9p^{(1-d_n)/2}/2 > 1$,

$$|\mathcal{C}_{d,n}| \geq D(p) p^{d_n^2/4 - 1/4}.$$

Since $|\mathrm{GL}(d, \mathbb{F}_p)| \leq p^{d^2}$, it follows that

$$\begin{aligned} 1 &\leq \frac{|\mathrm{GL}(d, \mathbb{F}_p)| \cdot |\mathfrak{C}_{d,n}|}{|\mathcal{C}_{d,n}|} \\ &\leq 1 + C(p)^2 D(p)\, p^{(d_n^2 - 2d_n + 2)/4 + d^2 - d_n^2/4 + 1/4} \\ &= 1 + K p^{d^2 - d_n/2}. \end{aligned}$$

If $n = 2$, then F_2/F_3 is an extension of $V \wedge V$ by V, and using the estimates of Lemma 6.3 and the argument above we obtain

$$\begin{aligned} 1 &\leq \frac{|\mathrm{GL}(d, \mathbb{F}_p)| \cdot |\mathfrak{C}_{d,n}|}{|\mathcal{C}_{d,n}|} \\ &\leq 1 + K p^{-d}. \end{aligned}$$

This proves part (a).

To prove part (b), we observe that $|\mathcal{C}_{d,n}| = \sum |\mathrm{GL}(d, \mathbb{F}_p)|/|\mathrm{GL}(d, \mathbb{F}_p)_{(w)}|$, where the sum is over all $\mathrm{GL}(d, \mathbb{F}_p)$-orbits in $\mathcal{C}_{d,n}$ and $|\mathrm{GL}(d, \mathbb{F}_p)_{(w)}|$ is the order of the stabilizer in $\mathrm{GL}(d, \mathbb{F}_p)$ of a typical element w of the orbit under consideration. Now $|\mathfrak{D}_{d,n}|$ is just the number of orbits for which $|\mathrm{GL}(d, \mathbb{F}_p)_{(w)}| = 1$, so

$$|\mathcal{C}_{d,n}| \leq |\mathrm{GL}(d, \mathbb{F}_p)| \cdot |\mathfrak{D}_{d,n}| + |\mathrm{GL}(d, \mathbb{F}_p)|(|\mathfrak{C}_{d,n}| - |\mathfrak{D}_{d,n}|)/2.$$

That is,

$$(2/|\mathrm{GL}(d, \mathbb{F}_p)|)|\mathcal{C}_{d,n}| - |\mathfrak{C}_{d,n}| \leq |\mathfrak{D}_{d,n}|,$$

so that

$$\begin{aligned} \frac{|\mathfrak{C}_{d,n}|}{|\mathfrak{D}_{d,n}|} &\leq \frac{|\mathfrak{C}_{d,n}|}{2|\mathcal{C}_{d,n}|/|\mathrm{GL}(d, \mathbb{F}_p)| - |\mathfrak{C}_{d,n}|} \\ &\leq \frac{|\mathfrak{C}_{d,n}| \cdot |\mathrm{GL}(d, \mathbb{F}_p)|/|\mathcal{C}_{d,n}|}{2 - |\mathfrak{C}_{d,n}| \cdot |\mathrm{GL}(d, \mathbb{F}_p)|/|\mathcal{C}_{d,n}|} \\ &\leq \frac{1 + K p^x}{1 - K p^x}. \end{aligned}$$

□

7 Summary

In this section we use Theorems 1.2, 1.3, and 1.4 to prove Theorem 1.1 along with two corollaries.

Theorem 1.1. *Fix a prime p and positive integers d and n. Let $r_{d,n}$ be the proportion of p-groups minimally generated by d elements and with lower p-length at most n whose automorphism group is a p-group. If $n \geq 2$, then*

$$\lim_{d\to\infty} r_{d,n} = 1.$$

If $d \geq 5$, then

$$\lim_{n\to\infty} r_{d,n} = 1.$$

If

$$n = 2 \text{ and } d \geq 10, \text{ or } n \geq 3 \text{ and } d \geq 6, \text{ or } n \geq 10 \text{ and } d \geq 5, \tag{9}$$

then

$$\lim_{p\to\infty} r_{d,n} = 1.$$

Proof. The set of p-groups minimally generated by d elements and with lower p-length at most n is $\mathfrak{A}_{d,n}$. When $n = 2$, $\mathfrak{A}_{d,n} = \mathfrak{C}_{d,n}$. The expression

$$C(p)^{n-1}D(p)^{n-2}p^{d_{n-1}-d_n/4+1/4+d^2}$$

goes to 0 as $d \to \infty$ if $n \geq 3$ or as $n \to \infty$ if $d \geq 5$. If d and n satisfy one of the conditions of Equation 9, then the exponent of p is negative. By Theorem 1.3, it follows that

$$\begin{aligned}
\lim_{d\to\infty} \frac{|\mathfrak{A}_{d,n}|}{|\mathfrak{C}_{d,n}|} &= 1 \quad \text{if } n \geq 2,\\
\lim_{n\to\infty} \frac{|\mathfrak{A}_{d,n}|}{|\mathfrak{C}_{d,n}|} &= 1 \quad \text{if } d \geq 5, \text{ and}\\
\lim_{p\to\infty} \frac{|\mathfrak{A}_{d,n}|}{|\mathfrak{C}_{d,n}|} &= 1 \quad \text{if one of the conditions in Equation 9 holds.}
\end{aligned}$$

The set $\mathfrak{D}_{d,n} \subseteq \mathfrak{C}_{d,n}$ is contained in the subset of $\mathfrak{A}_{d,n}$ of p-groups whose automorphism group is a p-group. By Theorem 1.4(b),

$$\begin{aligned}
\lim_{d\to\infty} \frac{|\mathfrak{C}_{d,n}|}{|\mathfrak{D}_{d,n}|} &= 1 \quad \text{if } n \geq 2,\\
\lim_{n\to\infty} \frac{|\mathfrak{C}_{d,n}|}{|\mathfrak{D}_{d,n}|} &= 1 \quad \text{if } d \geq 5, \text{ and}\\
\lim_{p\to\infty} \frac{|\mathfrak{C}_{d,n}|}{|\mathfrak{D}_{d,n}|} &= 1 \quad \text{if one of the conditions in Equation 9 holds.}
\end{aligned}$$

It follows that $|\mathfrak{A}_{d,n}|/|\mathfrak{D}_{d,n}|$ goes to 1 under the specified limits, and the theorem follows. □

Corollary 7.1. *Fix a prime p and $n \geq 2$. Let $s_{d,n}$ be the proportion of p-groups generated by at most d elements and with lower p-length at most n whose automorphism group is a p-group. Then*

$$\lim_{d\to\infty} s_{d,n} = 1.$$

Proof. This follows directly from Theorem 1.1 and the trivial observation that the number of p-groups generated by at most d elements and with lower p-length at most n is finite, while the number of p-groups with lower p-length at most n is infinite. □

Corollary 7.2. *Fix a prime p and $n \geq 2$. Let $t_{d,n}$ be the proportion of p-groups minimally generated by d elements and with lower p-length n whose automorphism group is a p-group. Then*

$$\lim_{d\to\infty} t_{d,n} = 1.$$

Proof. As $\mathfrak{D}_{d,n} \subseteq \mathfrak{B}_{d,n} \cup \{F_n/F_{n+1}\} \subseteq \mathfrak{A}_{d,n}$, it follows from Theorem 1.1 that

$$\lim_{d\to\infty} \frac{|\mathfrak{B}_{d,n}| + 1}{|\mathfrak{D}_{d,n}|} = 1.$$

Since $|\mathfrak{A}_{d,n}| \to \infty$ as $d \to \infty$, Theorem 1.1 implies that $|\mathfrak{D}_{d,n}| \to \infty$ as $d \to \infty$, proving that

$$\lim_{d\to\infty} \frac{|\mathfrak{B}_{d,n}|}{|\mathfrak{D}_{d,n}|} = 1.$$

□

Using Theorem 1.1, Henn and Priddy [12] prove the following theorem.

Theorem 7.3 (Henn and Priddy [12]). *Fix a prime p and integers $d, n \geq 2$. Let $u_{d,n}$ be the proportion of p-groups P generated by at most d elements and with lower p-length at most n that satisfy the following property: if H is a finite group with Sylow p-subgroup P, then H has a normal p-complement. Then* $\lim_{d\to\infty} u_{d,n} = 1$.

As mentioned in the introduction, the following question remains unanswered.

Question. *Fix a prime p. Let v_n be the proportion of p-groups with order at most p^n whose automorphism group is a p-group. Is it true that* $\lim_{n\to\infty} v_n = 1$*?*

8 Acknowledgements

We would like to thank Persi Diaconis for introducing us to each other and for his continued support of this project. We would also like to thank Charles Leedham-Green for several illuminating conversations and for his help with the examples in the introduction. Finally, we would like to thank Eamonn O'Brien for his help with references and computational data. For part of this research, the first author was supported by a Department of Defense National Defense Science and Engineering Graduate Fellowship.

References

[1] H. U. Besche, B. Eick, and E. A. O'Brien, *A millennium project: constructing small groups*, Internat. J. Algebra Comput. **12** (2002), no. 5, 623–644.

[2] G. Birkhoff, *Subgroups of abelian groups*, Proc. London Math. Soc. (2) **38** (1934–35), 387–401.

[3] R. M. Bryant and L. G. Kovács, *Lie representations and groups of prime power order*, J. London Math. Soc. (2) **17** (1978), 415–421.

[4] B. Eick, C. R. Leedham-Green, and E. A. O'Brien, *Constructing automorphism groups of p-groups*, Comm. Algebra **30** (2002), no. 5, 2271–2295.

[5] B. Eick and E. A. O'Brien, *Enumerating p-groups*, J. Austral. Math. Soc. Ser. A **67** (1999), no. 2, 191–205.

[6] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*, 2005, packages AutPGrp and SmallGroups (`http://www.gap-system.org`).

[7] A. M. Garsia, *Combinatorics of the free Lie algebra and the symmetric group*, Analysis, et cetera, Academic Press, Boston, MA, 1990, pp. 309–382.

[8] J. A. Gibbs, *Automorphisms of certain unipotent groups*, J. Algebra **14** (1970), 203–228.

[9] J. Goldman and G.-C. Rota, *On the foundations of combinatorial theory. IV. Finite vector spaces and Eulerian generating functions*, Studies in Appl. Math. **49** (1970), 239–258.

[10] P. Hall, *A contribution to the theory of groups of prime-power order*, Proc. London Math. Soc. **36** (1934), 29–95.

[11] G. T. Helleloid, *A survey on automorphism groups of finite p-groups*, available at arXiv:math.GR/0610294.

[12] H.-W. Henn and S. Priddy, *p-nilpotence, classifying space indecomposability, and other properties of almost all finite groups*, Comment. Math. Helv. **69** (1994), no. 3, 335–350.

[13] G. Higman, *Enumerating p-groups. I. Inequalities*, Proc. London Math. Soc. (3) **10** (1960), 24–30.

[14] M. V. Horoševskiĭ, *The automorphism groups of finite p-groups*, Algebra i Logika **10** (1971), 81–86, English translation in Algebra and Logic **10** (1971), 54–57.

[15] ———, *The automorphism group of wreath products of finite groups*, Sibirsk. Mat. Ž. **14** (1973), 651–659, 695, English translation in Siberian Math. J. **14** (1973), 453–458.

[16] B. Huppert and N. Blackburn, *Finite groups. II*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 242, Springer-Verlag, Berlin, 1982.

[17] M. Lazard, *Sur les groupes nilpotents et les anneaux de Lie*, Ann. Sci. Ecole Norm. Sup. (3) **71** (1954), 101–190.

[18] A. Lubotzky and D. Segal, *Subgroup growth*, Progress in Mathematics, vol. 212, Birkhäuser Verlag, Basel, 2003.

[19] I. G. Macdonald, *Symmetric functions and Hall polynomials*, second ed., Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1995.

[20] A. Mann, *Some questions about p-groups*, J. Austral. Math. Soc. Ser. A **67** (1999), no. 3, 356–379.

[21] U. Martin, *Almost all p-groups have automorphism group a p-group*, Bull. Amer. Math. Soc. (N.S.) **15** (1986), no. 1, 78–82.

[22] H. Neumann, *Varieties of groups*, Springer-Verlag New York, Inc., New York, 1967.

[23] M. F. Newman, *Determination of groups of prime-power order*, Group theory (Proc. Miniconf., Australian Nat. Univ., Canberra, 1975), Springer, Berlin, 1977, pp. 73–84. Lecture Notes in Math., Vol. 573.

[24] M. F. Newman and E. A. O'Brien, *A CAYLEY library for the groups of order dividing* 128, Group Theory (Singapore, 1987), de Gruyter, Berlin, 1989, pp. 437–442.

[25] E. A. O'Brien, *The p-group generation algorithm*, J. Symbolic Comput. **9** (1990), no. 5-6, 677–698, Computational group theory, Part 1.

[26] ———, *Computing automorphism groups of p-groups*, Computational algebra and number theory (Sydney, 1992), Math. Appl., vol. 325, Kluwer Acad. Publ., Dordrecht, 1995, pp. 83–90.

[27] C. Reutenauer, *Free Lie algebras*, London Mathematical Society Monographs. New Series, vol. 7, The Clarendon Press Oxford University Press, New York, 1993.

[28] C. C. Sims, *Enumerating p-groups*, Proc. London Math. Soc. (3) **15** (1965), 151–166.

[29] A. I. Skopin, *The factor groups of an upper central series of free groups*, Doklady Akad. Nauk SSSR (N.S.) **74** (1950), 425–428.

[30] U. H. M. Webb, *The occurrence of groups as automorphisms of nilpotent p-groups*, Arch. Math. (Basel) **37** (1981), no. 6, 481–498.

[31] E. T. Whittaker and G. N. Watson, *A course of modern analysis*, Fourth edition. Reprinted, Cambridge University Press, New York, 1962.

[32] H. S. Wilf, *Three problems in combinatorial asymptotics*, J. Combin. Theory Ser. A **35** (1983), no. 2, 199–207.

[33] D. L. Winter, *The automorphism group of an extraspecial p-group*, Rocky Mountain J. Math. **2** (1972), no. 2, 159–168.